PGP CORPORATION

PGP 8.0 FOR WINDOWS

User's Guide

Version Information

PGP 8.0.1 User's Guide. Released February 2003.

Copyright Information

Copyright © 1991-2003 by PGP Corporation. All Rights Reserved. No part of this document can be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PGP Corporation.

Trademark Information

PGP and Pretty Good Privacy are registered trademarks of PGP Corporation in the U.S. and other countries. IDEA is a trademark of Ascom Tech AG. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST encryption algorithm is licensed from Northern Telecom, Ltd. PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

The compression code in PGP is by Mark Adler and Jean-Loup Gailly, used with permission from the free Info-ZIP implementation. This software is based in part on the work of the Independent JPEG Group. Soft TEMPEST font courtesy of Ross Anderson and Marcus Kuhn. Biometric word list for fingerprint verification courtesy of Patrick Juola.

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restrict the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

About PGP Corporation

PGP Corporation, the recognized worldwide leader in secure messaging and data storage, builds products that allow corporations to ensure confidential customer and individual information remains secure. Over the past 12 years, PGP technology has developed a global reputation for enabling open, trusted, and highly reliable security products. PGP has thousands of corporate/government users and millions of individual users worldwide, including many of the world's largest and most security sensitive enterprises, government agencies, individuals, and cipher experts. Contact PGP Corporation at www.pgp.com.

Table of Contents

Introduction 7

Who should read this User's Guide 7

Licensing 7

This User's Guide. 9

Recommended readings 10

Symbols 12

Chapter 1: PGP Basics **13**

Overview 13

Conventional and public-key cryptography 13

So what is PGP really? 14

This user's guide. 14

Basic steps for using PGP 15

Chapter 2: The PGP Interface **17**

Overview 17

Accessing PGP 17

PGP Screens. 21

Chapter 3: Making a Keypair and Working with Public Keys **23**

Making your keypair 23

Putting your public key on a keyserver 25

Getting someone's public key from a keyserver. 26

Chapter 4: Securing Email **27**

Encrypting and signing email 27

Decrypting and verifying email. 34

PGP/MIME. 36

Chapter 5: Securing Files **37**

Securing your files and folders with PGP 37

Signing and decrypting files with a split key 39

Permanently erasing files and free disk space. . . . 39

Chapter 6: Wiping . . . 45

Overview . . . 45

Using PGP Wipe to permanently delete a file. . . . 45

Using the Wipe Free Space Wizard to clean free disk space . . . 46

Scheduling folder and free space wiping . . . 49

Chapter 7: Self-Decrypting Archives. . . . 53

Creating an SDA . . . 53

Opening an SDA . . . 54

Chapter 8: Securing ICQ . . . 55

About ICQ. . . . 55

Exchanging public keys in ICQ . . . 56

Encrypting ICQ messages. . . . 59

Chapter 9: Using Lotus Notes . . . 61

Overview . . . 61

Encrypting and signing. . . . 61

Decrypting and verifying . . . 63

Chapter 10: Using Smart Cards . . . 65

Overview . . . 65

Generating a keypair on a smart card . . . 66

Examining smart card properties . . . 68

Copying your public key from a smart card to someone's keyring . . . 69

Wiping keys from your smart card . . . 70

Copying a keypair from your keyring to a smart card . . . 71

Chapter 11: PGP Disk Basics . . . 73

What is PGP Disk?. . . . 73

Accessing PGPdisk . . . 73

Working with PGPdisk in Windows Explorer . . . 74

Creating a new PGPdisk volume . . . 75

Mounting a PGPdisk volume . . . 78

Using a mounted PGPdisk volume . . . 78
Unmounting a PGPdisk volume . . . 79

Chapter 12: Using PGP Disk . . . 81
Working with PGPdisk in a PGPdisk Editor . . . 81
Maintaining PGPdisk volumes . . . 86

Chapter 13: PGP Disk Technical Details . . . 91
About PGPdisk volumes . . . 91
The PGPdisk encryption algorithms . . . 91
Special security precautions taken by PGPdisk . . . 92

Chapter 14: Making Keys . . . 95
Choosing a key type . . . 95
Making a keypair . . . 96
Generating a custom key . . . 99
Adding your email ID from your Microsoft Exchange Server to your new key . . . 102
Creating a passphrase you will remember . . . 103
Changing your keypair . . . 103
Protecting your keys . . . 104
PGP key reconstruction . . . 104

Chapter 15: Exchanging Keys . . . 107
Overview . . . 107
Distributing your public key . . . 107
Obtaining the public keys of others . . . 110
Validating keys . . . 112

Chapter 16: Managing Keys . . . 113
Overview . . . 113
The PGPkeys screen . . . 114
PGPkeys attribute definitions . . . 115
Specifying a default keypair on your PGP keyring . . . 118
Importing and exporting keys on your PGP keyring . . . 119
Deleting a key or signature on your PGP keyring . . . 119

Disabling and enabling keys on your PGP keyring 119
Examining and setting key properties 120
General key properties 120
Subkeys properties 127
Designated revoker properties. 129
Additional Decryption Key properties 131
Adding an X.509 certificate to your PGP key 132
Splitting and rejoining keys 135
Updating your key on a keyserver 141
Reconstructing your key 143

Appendix A: Setting PGP Options 145
About PGP Options 145
Setting General options 145
Setting Files options 148
Setting Email options 149
Setting HotKeys options. 150
Setting Servers options 151
Setting certificate authority (CA) options 154
Setting Advanced options 155
Setting PGP Disk options. 158

Appendix B: Troubleshooting. 161

Appendix C: Biometric Word Lists. 165

Glossary 171

Index 181

Introduction

This User's Guide explains how to use PGP 8.0.

Who should read this User's Guide

This User's Guide is for anyone who is going to be using the PGP 8.0 software to protect their data.

Note: If you are new to cryptography and would like an overview of the terminology and concepts in PGP, please refer to *An Introduction to Cryptography* (it was put onto your computer when you installed PGP 8.0).

Licensing

PGP uses a license number system to determine what PGP features will be active on your computer. Following is a brief description of that system. For complete information and purchase options, go to https://store.pgp.com.

Licensing options

When you start PGP for the first time after installation, the PGP License screen appears. You have two options: you can enter your PGP license information (there are two ways of doing this, described below) or you can use PGP unlicensed for non-commercial use only; this is called PGP Freeware.

Warning: Commercial use of PGP Freeware is a violation of the License Agreement.

If you choose the second option, PGP Freeware (and you are legally permitted to do so under the end-user license agreement for non-commercial use), then you will be able to use PGPmail, PGPkeys, and PGPtray. The PGP email plugins and PGPdisk will not be available.

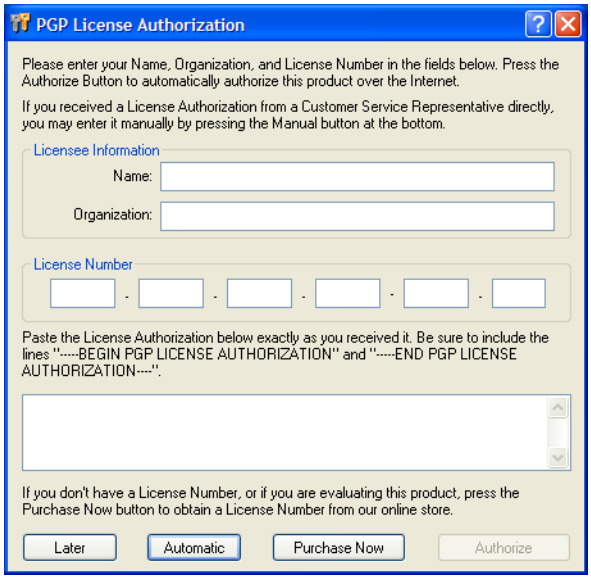
If you use a licensed version of PGP, the functionality that will be available depends on the type of license you purchased:

- **Personal:** includes support for PGPmail, PGPkeys, PGPtray, PGPdisk, and the personal email plugins—Eudora, ICQ, Outlook Express, and Outlook. Although the Outlook plugin will be installed, you will not be able to use it if you have configured Exchange Server accounts.
- **Desktop:** includes support for PGPmail, PGPkeys, PGPtray, PGPdisk, and all email plugins—the personal email plugins plus GroupWise, Lotus Notes, and support for Exchange Server environments in Outlook.
- **Enterprise:** includes support for all PGP functionality mentioned above, plus PGPadmin and PGP Keyserver.

Entering your license information

There are two ways to enter your PGP license information:

- If you have your License Number and an active Internet connection, enter your License Number in the appropriate box on the PGP License screen. Also enter a Name and Organization to associate with the License Number. Make sure to remember (or write down) the Name and Organization you enter, because PGP will save this information and if you need to authorize again, you will need to enter the Name and Organization exactly as you entered it the first time. When all three boxes are filled in, click **Authorize**.


PGP License Authorization
Please enter your Name, Organization, and License Number in the fields below. Press the Authorize Button to automatically authorize this product over the Internet.
If you received a License Authorization from a Customer Service Representative directly, you may enter it manually by pressing the Manual button at the bottom.
Licensee Information
Name:
Organization:
License Number
Paste the License Authorization below exactly as you received it. Be sure to include the lines "-----BEGIN PGP LICENSE AUTHORIZATION" and "-----END PGP LICENSE AUTHORIZATION-----".
If you don't have a License Number, or if you are evaluating this product, press the Purchase Now button to obtain a License Number from our online store.
Later
Automatic
Purchase Now
Authorize

- If you are unable to Authorize automatically using the above method and you have been sent a License Authorization from PGP Customer Service, click **Manual**, paste the license authorization block into the box, then click **Authorize**.

This User's Guide

The chapters and appendices in this User's Guide include:

- Chapter 1, PGP Basics, provides an overview of PGP and what it does.
- Chapter 2, The PGP Interface, describes and shows the way you interact with PGP.
- Chapter 3, Making a Keypair and Working with Public Keys, tells you how to make your first keypair and how to upload your public key to a keyserver and how to download the public keys of others.
- Chapter 4, Securing Email, tells you how to use PGP to secure your email messages.
- Chapter 5, Securing Files, tells you how to use PGP to secure files on your computer.
- Chapter 6, Wiping, describes how to erase files and/or folders from your system so that they are not recoverable.
- Chapter 7, Self-Decrypting Archives, describes self-decrypting archives (SDAs) and tells you how to create them.
- Chapter 8, Securing ICQ, tells you how to secure your ICQ communications.
- Chapter 9, Using Lotus Notes, describes the Lotus Notes plugin and tells you how to use it.
- Chapter 10, Using Smart Cards, describes smart cards and tells you how to use them with PGP.
- Chapter 11, PGP Disk Basics, provides an overview of PGP Disk.
- Chapter 12, Using PGP Disk, tells you how to use PGP Disk.
- Chapter 13, PGP Disk Technical Details, describes technical details behind PGP Disk.
- Chapter 14, Making Keys, tells you how to create PGP keys.
- Chapter 15, Exchanging Keys, tells you how to exchange PGP keys with others.
- Chapter 16, Managing Keys, tells you how to manage your PGP keys.
- Appendix A, Setting PGP Options, describes PGP's options.
- Appendix B, Troubleshooting, tells you how to fix problems you may run into.
- Appendix C, Biometric Word Lists, tells you about PGP's special biometric word lists and what they're for.

There is also a Glossary and an Index.

Recommended readings

This section identifies Web sites, books, and periodicals about the history, technical aspects, and politics of cryptography, as well as trusted PGP download sites.

The history of cryptography

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.
- *The Codebreakers: The Story of Secret Writing*, David Kahn, Simon & Schuster Trade, 1996, ISBN 0-684-83130-9 (updated from the 1967 edition). This book is a history of codes and code breakers from the time of the Egyptians to the end of WWII. Kahn first wrote it in the sixties; this is the revised edition. This book won't teach you anything about how cryptography is done, but it has been the inspiration of the whole modern generation of cryptographers.

Technical aspects of cryptography

Web sites

- www.iacr.org. International Association for Cryptologic Research (IACR). The IACR holds cryptographic conferences and publishes journals.
- www.pgpi.org. An international PGP Web site, which is not maintained by PGP Corporation, is an unofficial yet comprehensive resource for PGP.
- www.nist.gov/aes. The National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) Development Effort, perhaps the most interesting project going on in cryptography today.
- www.ietf.org/rfc/rfc2440.txt. The specification for the IETF OpenPGP standard.

Books and periodicals

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. If you can only buy one book to get started in cryptography, this is the one to buy.
- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot and Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. This is the technical book you should get after Schneier. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.
- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). See www.iacr.org.

- *Advances in Cryptology*, conference proceedings of the IACR CRYPTO conferences, published yearly by Springer-Verlag. See www.iacr.org.
- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (introductory tutorial article).
- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Contains details about the Twofish cipher ranging from design criteria to cryptanalysis of the algorithm.

Politics of cryptography

Web sites

- www.epic.org, Electronic Privacy Information Center.
- www.crypto.org, Internet Privacy Coalition.
- www.eff.org, Electronic Frontier Foundation.
- www.privacy.org, privacy.org. Great information resource about privacy issues.
- www.cdt.org, Center for Democracy and Technology.
- www.philzimmermann.com, Phil Zimmermann's home page, his Senate testimony, and so on.

Books

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie and Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don't know.
- *Technology and Privacy: The New Landscape*, Philip Agre and Marc Rotenberg, The MIT Press, 1997;ISBN 0-262-01162-x.
- *Building in Big Brother, The Cryptographic Policy Debate*, edited by Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

Network security

Books

- *Building Internet Firewalls*, Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper, and Deborah Russell (Editor), O'Reilly & Associates, Inc., 2000; ISBN: 1565928717. This book is a practical guide to designing, building, and maintaining firewalls.
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, Inc., 1994; ISBN: 0201633574. This book is a practical guide to protecting networks from hacker attacks through the Internet.
- *Hacking Exposed: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray, and George Kurtz, The McGraw-Hill Companies, 1999; ISBN: 0072121270. The state of the art in breaking into computers and networks, as viewed from the vantage point of the attacker and the defender.

Symbols

Notes, Cautions, and Warnings are used in the following ways.

Notes are extra, but important, information.

Note: A Note adds important information, but you could still use the product if you didn't have that information.

Cautions indicate the possibility of loss of data or minor damage to equipment.

Caution: A Caution tells you about a situation where there is the potential for loss of data or minor damage to equipment. Special attention should be paid to Cautions.

Warnings indicate the possibility of significant damage to equipment or injury to human beings.

Warning: A Warning means that your equipment may be damaged or a person could be injured. Please take Warnings seriously.

1 PGP Basics

This chapter introduces you to PGP, Pretty Good Privacy.

The sections in this chapter are:

- Overview
- Conventional and public-key cryptography
- So what is PGP really?
- This user's guide
- Basic steps for using PGP

Overview

PGP is a tool for keeping your data safe. It encrypts (scrambles) your data so that if an unauthorized person gets hold of it, they can't make heads or tails of it. Naturally, when you want to use it, it gets changed back to normal (decrypted).

For lots of information about encryption, see *An Introduction to Cryptography*, which was installed on your computer when PGP was installed.

Conventional and public-key cryptography

There are two kinds of cryptography (the science that includes encryption): conventional and public-key.

Conventional cryptography uses the same passphrase to encrypt and decrypt data. Conventional cryptography is great for data that isn't going anywhere. However, conventional cryptography isn't as well suited for situations where you need to send encrypted data to someone else or if you want to send encrypted data to someone you've never met.

Fortunately, public-key cryptography is especially well suited to these two situations. Public-key cryptography uses two keys (called a keypair) for encrypting and decrypting. One of these two keys is called your private key; and like the name suggests, you need to keep it private. Very, very private. The other key is called your public key, and like its name suggest, you can share it with the general public. In fact, you're supposed to share it.

Caution: Don't give your private key, or its passphrase, to anyone.

(Technical note: your public and private keys are mathematically related, but there's no way to figure out someone's private key if you just have their public key.)

So how does public-key cryptography work? Let's say you and your cousin in another state want to exchange private messages. Both of you have PGP. First, you both need to create your keypair: one private key and one public key. Your private key you keep secret, your public key you send to a public keyserver, which is a public facility for distributing public keys. (Some companies have their own private keyservers.)

Once the public keys are on the keyserver, you can go back to the keyserver and get your cousin's public key, and she can go to the keyserver and get yours. This is important because to send an encrypted email message that only your cousin can decrypt, you encrypt it using your cousin's public key. What makes this work is that only your cousin's private key can decrypt a message that was encrypted using her public key. Even you, who have her public key, can't decrypt the message once it's been encrypted using her public key.

Let's be very clear about this: **only a private key can decrypt data that was encrypted with the corresponding public key.**

So to send a private message that only you can decrypt and read, your cousin encrypts it with your public key. Your private key is the only key in the world that can decrypt that message; and of course you're keeping your private key very, very private, right?

So what is PGP really?

PGP is a tool for keeping your data safe. It has three main components:

- **PGPkeys**: Create your personal keypair (a private key and a public key) and get and manage the public keys of other people.
- **PGPmail**: Encrypt email messages to other people and decrypt email messages sent to you.
- **PGPdisk**: Encrypt a portion of your hard disk so that it's fully protected even if it's stolen.

PGP also does things like secure your ICQ communications, wipe files so that they are completely gone, and create self-decrypting archives.

This user's guide

This user's guide describes all three of these components of PGP, but in a slightly different order than you might think. First we talk about creating your keypair and sending your public key to a keyserver; this should be a part of the PGP Keys section, but because most things you do with PGP requires a keypair, we cover it first.

Then we talk about PGP Mail, then PGP Disk, and then we come back to PGP Keys.

Basic steps for using PGP

Now that we know a little bit about PGP, let's go deeper into what you need to do to get started using PGP:

1. Install PGP on your computer.

   If you are a corporate user, your corporate or PGP administrator may have specific installation instructions for you to follow, or your company may install the product on your machine for you. Either way, this is the first step.

2. Create your keypair.

   As mentioned earlier, most things you do with PGP require a keypair (a private key and a public key). If you haven't created your keypair yet, or you have but you're still new to PGP, see Chapter 3, Making a Keypair and Working with Public Keys for instructions how to create your keypair.

3. Exchange public keys with others.

   After you have created a keypair, you can begin corresponding with other PGP users. You will need a copy of their public key and they will need yours.

   We cover this briefly in Chapter 3, Making a Keypair and Working with Public Keys, and you can also see Chapter 15, Exchanging Keys for detailed information.

4. Validate the public keys you get from the keyserver.

   Once you have a copy of someone's public key, you can add it to your public keyring. A keyring is a file that stores your keys. Each user has two keyrings: one public and one private. Your public keyring stores public keys; yours, and those you receive from others. Your private keyring stores your private key(s).

   When you get someone's public key, you should make sure that it has not been tampered with and that it really belongs to the purported owner. You do this by comparing the unique fingerprint on your copy of someone's public key to the fingerprint on that person's original key.

   For more information about validity and trust, refer to *An Introduction to Cryptography*. For instructions how to validate someone's public key, see "Validating keys" on page 112.

5. Start securing your email and files.

   After you have generated your keypair and have exchanged public keys, you can begin encrypting, signing, decrypting and verifying your email messages and files.

   To perform a PGP task, you must select the file or email message that you want to secure and then choose your task (Encrypt, Sign, Decrypt, or Verify). To learn how to access PGP, see Chapter 2, The PGP Interface.

2 The PGP Interface

This chapter shows and describes the PGP interface.

Overview

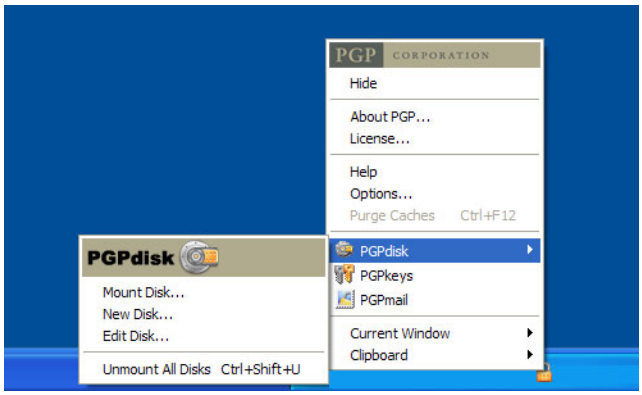
There are multiple ways to access PGP functions, depending on what you want to do. This chapter shows and describes ways to access PGP and PGP's main screens: PGP Keys, PGP Mail, and the PGP Disk Editor.

Accessing PGP

There are four main ways to access PGP: via the PGPtray icon, via the Start Menu, via Windows Explorer, and from within some email applications.

The PGPtray icon

One way to access many PGP features is from the PGPtray icon.



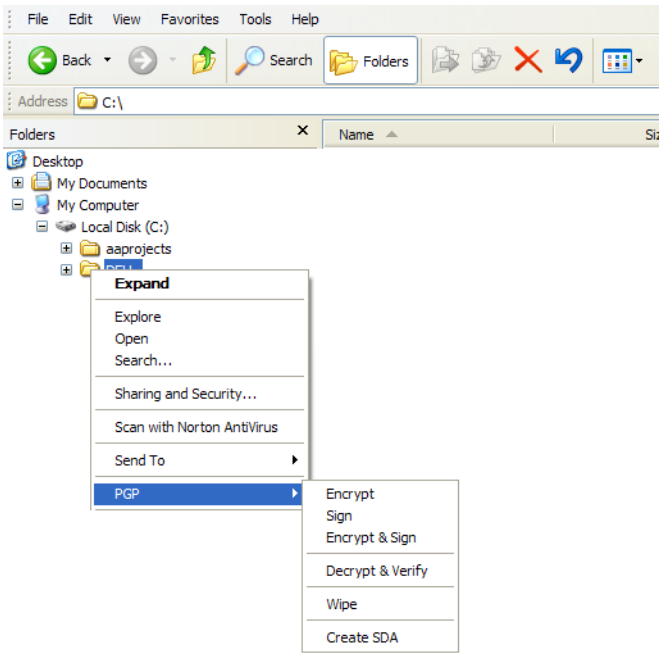
When you click on the PGP icon in the Windows System tray (we call this the PGPtray icon), a menu appears giving you access to:

- The About PGP screen, which displays information about the version of PGP you are using, including the licensing information
- PGP online help, so that you have easy access to information about PGP
- PGP options, so that you can control your PGP environment
- Purging passphrase caches, so that can remove stored passphrases from the cache to prevent unauthorized use of PGP

- PGP Disk functions, so that you have quick access to PGPdisk functionality
- The PGP Keys and PGP Mail screens, so that you have easy access to PGPkeys and PGPmail functionality
- Encrypt, decrypt/verify, and sign options for data in the Current Window, so that you can use PGP on the current window
- Empty, Edit, encrypt, decrypt/verify, and sign options for data on the Clipboard, so that you can use PGP on the contents of the Clipboard

Windows Explorer

You can also access PGP functions from Windows Explorer. Simply open Windows Explorer and then select the items you want to work on.



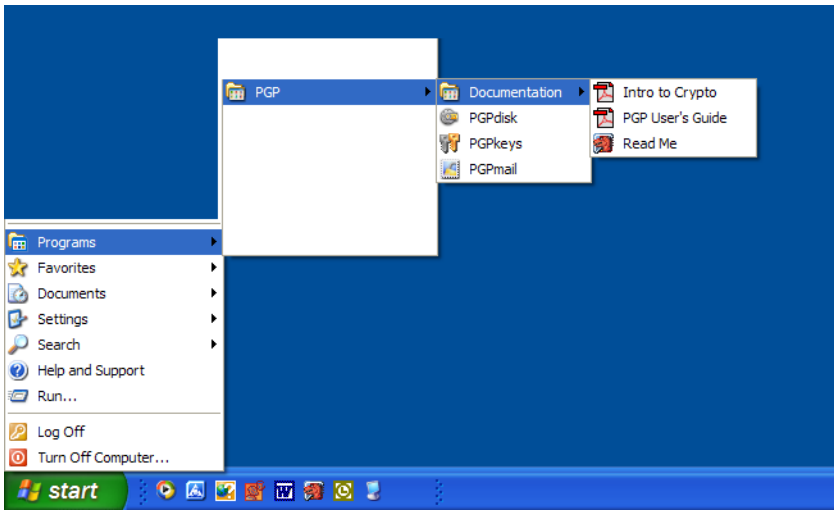
Windows Explorer gives you access to different PGP functions depending on what you select:

- **Drive**. If you right click a drive on your system in Windows Explorer and select PGP from the menu that appears, you can do the following to the drive:
  - Encrypt, Sign, or Encrypt & Sign it
  - Decrypt & Verify it
  - Wipe free space on it
  - Create a self-decrypting archive (SDA) of the drive

- **Folder.** If you right click a folder in Windows Explorer and select PGP from the menu that appears, you can do the following to the folder:
  - Encrypt, Sign, or Encrypt & Sign it
  - Decrypt & Verify it
  - Wipe it
  - Create an SDA with the contents of the folder in the archive
- **File**. If you right-click a file in Windows Explorer, the PGP submenu lets you perform various functions on the file, depending on what kind of file it is:
  - If you select an unencrypted file, you can encrypt, sign, wipe, or create an SDA
  - If you select an encrypted file, you can decrypt/verify or wipe it
  - If you select a PGPdisk file (.pgd), you can mount or edit it
  - If you select an ASCII key file (.asc), you can decrypt/verify or wipe it. If you select decrypt/verify, you are given the option of importing the file.
  - If you select a PGP public or private keyring file (.pkr or .skr, respectively), you can add the keys in it to your keyring or wipe the file

The Start Menu

Another way to access PGP is through the Windows Start Menu. Click **Start,** slide up to **Programs**, then over to **PGP**.

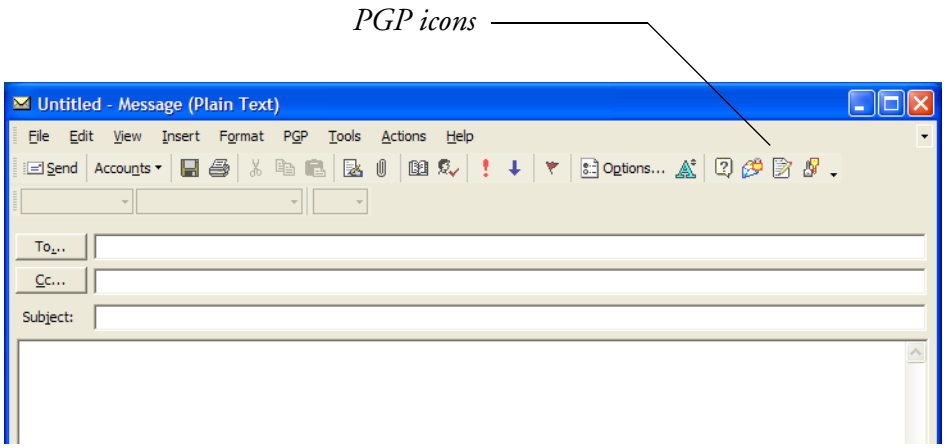


The Start Menu gives you access to:

- PGP documentation
- PGP Disk functions
- The PGP Keys and PGP Mail screens

Email applications

You can access some PGP functions from within certain email applications, like Microsoft Outlook, for example.



If you are creating a new message in Outlook, the Standard toolbar will have PGP icons that let you:

- Encrypt the message
- Sign the message
- Open PGP Keys

The Outlook Inbox also has PGP icons for:

- Decrypting a message and verifying its signature
- Opening PGP Keys

PGP installs PGP icons into the following email applications:

- Microsoft Exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes
- Novell GroupWise
- QUALCOMM Eudora

Note: If you use an email application that doesn't have PGP icons on its toolbar, you can use the PGPtray icon to perform PGP functions on either the Current Windows or the Clipboard.

Be sure to check the toolbar of your email application for the PGP icons.

PGP Screens

PGP's main screens are those for PGP Keys, PGP Mail, and the PGP Disk Editor.

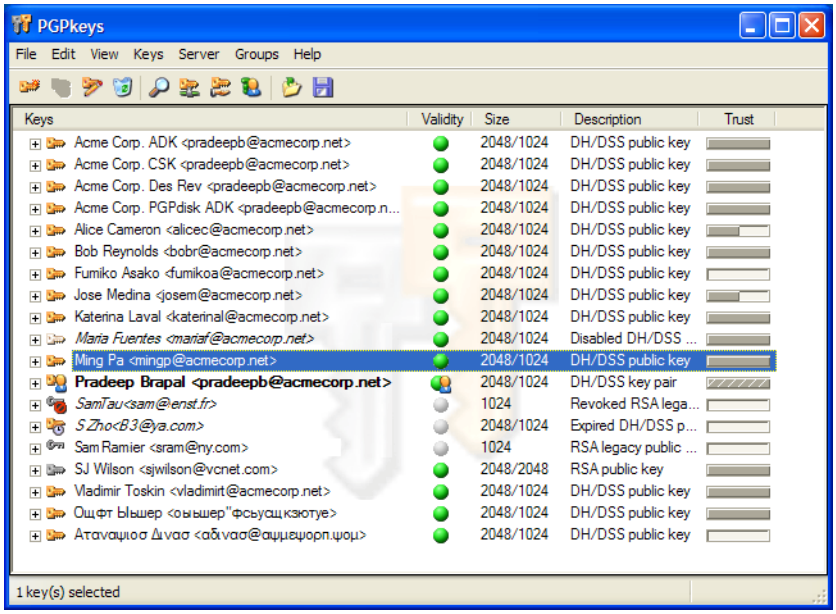
The PGP Keys Screen

The PGP Keys screen lets you manage your public/private keypair(s) and the public keys of others. For more detailed information about managing keys, refer to Chapter 16, Managing Keys.

To access the PGP Keys screen:

1. Click the PGPtray icon.
2. Select PGPkeys from the menu.

   The PGPkeys screen appears.



The PGP Mail Screen

The PGP Mail screen gives you quick access to basic PGP functions: encrypt, sign, encrypt and sign, decrypt/verify, wipe, and freespace wipe. You can also open the PGPkeys screen. For more information about PGPmail functionality, refer to Chapter 4, Securing Email and Chapter 5, Securing Files.

To access the PGP Mail screen:

1. Click the PGPtray icon.
2. Select PGPmail from the menu.

   The PGPmail screen appears.

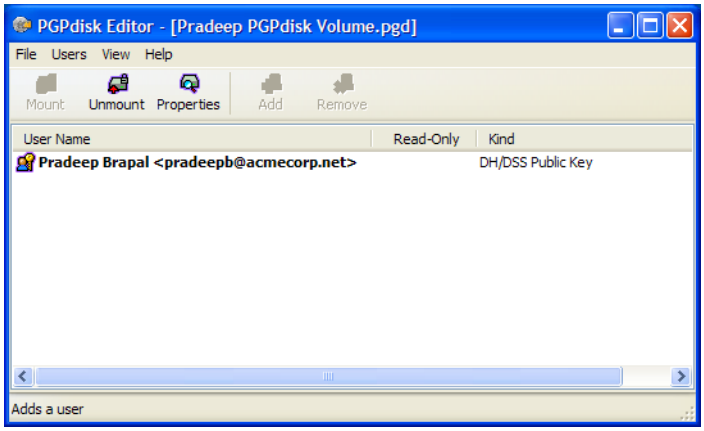
The PGP Disk Editor Screen

The PGP Disk Editor screen lets you do things to PGPdisk volumes like change the passphrase or add alternate users.

You can access the PGP Disk Editor screen in either of the following ways:

- Click the **PGPtray icon**, slide up to **PGPdisk** and then over to **Edit Disk**. On the Choose a PGPdisk screen, select the PGPdisk you want to open, then click **Open**.
- In Windows Explorer, right click on the PGPdisk you want to edit, slide down to **PGP**, then over to **Edit PGPdisk**.

  The PGPdisk Editor screen appears for the selected PGPdisk.



3 Making a Keypair and Working with Public Keys

This chapter describes three things that first-time PGP users should consider doing soon after they install PGP: creating their public/private keypair, sending their public key to a key server, and getting the public keys of others from a key server.

If you have a public/private keypair and you've worked with public key servers before, then you can probably skip this chapter.

The sections in this chapter are:

- Making your keypair
- Putting your public key on a keyserver
- Getting someone's public key from a keyserver

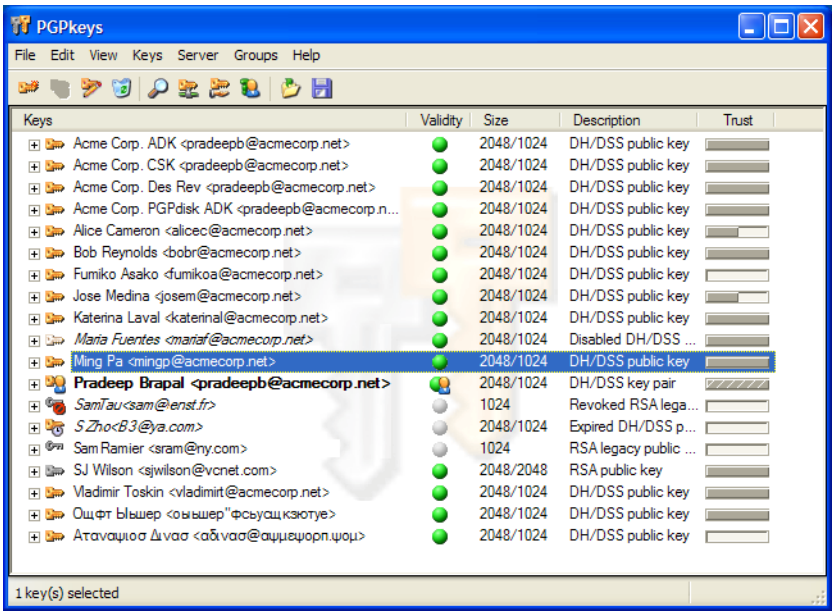
Making your keypair

To create a new keypair:

1. Open PGPkeys. You can open PGPkeys by:
   - Clicking **Start—>Programs—>PGP—>PGPkeys**
   - Clicking the PGPtray icon ( ) in the System tray, then selecting **PGPkeys**

   The PGPkeys screen displays the keypairs you have created for yourself, as well as any public keys of other users that you have added to your public keyring. PGPkeys is your tool for managing your keyrings.

Note: Depending on your situation, the PGPkeys window may be empty, or it may be pre-configured by your PGP administrator to display specific keys.



2. Click in the PGPkeys menu bar or pull down the **Keys** menu and select **New Key**.

   The PGP Key Generation Wizard provides some introductory information on the first screen.

3. After you read the information, click **Next**.

   The PGP Key Generation Wizard asks you to enter your name and email address.

4. Enter your name in the **Full Name** box and your email address in the **Email Address** box, then click **Next**.

   It is not absolutely necessary to enter your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and others can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient.

5. If PGP detects that your computer is in a Microsoft Exchange Server environment or if your PGP administrator has configured PGP to include specific installation settings, the **Administrator Options** panel appears. Read the information on this panel, then click **Next** to continue.

6. On the **Passphrase** screen, enter the string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press Tab to advance to the next field, then enter the same passphrase again. For more information on creating an effective passphrase, see "Creating a passphrase that you will remember" on page 45.

Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the **Hide Typing** check box.

Caution: Unless your administrator has implemented a PGP key reconstruction policy for your company, no one, including PGP Corporation, can salvage a key with a forgotten passphrase.

7. Click **Next** to begin the key generation process.

   Your mouse movements and keystrokes generate random information that is needed to create a unique keypair. If there is not enough random information upon which to build the key, the **PGP Random Data** dialog box appears. As instructed in the dialog box, move your mouse around and enter a series of random keystrokes until the progress bar is completely filled in.

   If you are in a Microsoft Exchange Server environment, PGP informs you that it needs to retrieve your email user ID from your Exchange server in order to add it to your new PGP key. If this is the case, continue with the instructions outlined in "Adding your email ID from your Microsoft Exchange Server to your new key" on page 43.

8. When the key generation process indicates that it is done, click **Next**.
9. Click **Finish**.

Putting your public key on a keyserver

The best method for making your public key available is to place it on a public keyserver, which is a large database of keys that anyone can access. That way, people can send you encrypted email without having to get your public key from you.

To put your public key on a keyserver:

1. Open PGP Keys.

   The PGP Keys screen appears.

2. Pull down the **Server** menu, select **Send To**, then slide over and down to the keyserver of your choice.

   Your public key is uploaded to the keyserver you selected.

Getting someone's public key from a keyserver

For you to send an encrypted email message to someone else, you need to get their public key first.

To get someone's public key from a keyserver:

1. Open PGPkeys.
2. Choose **Search** from the **Server** menu or click the **Search** button in PGPkeys.

   The PGPkeys Search Window screen appears.
3. Choose the server you wish to search from the **Search for keys on** drop-down menu.
4. Specify your search criteria.

   For example: User ID contains John Galt

   This would find the keys with the name John Galt in their user ID.
5. Click **More Choices** to add additional criteria to your search; for example, Key IDs with the name Susan Jones created on or before March 6, 1982.
6. Click **Search**.

   A progress bar appears displaying the status of the search. To cancel a search in progress, click **Stop Search**.

   The results of the search appear in the window.
7. To import a key, drag it from the search window onto the PGP Keys window and drop it there.

   You can import multiple keys at one time if you wish.
8. Close the PGPkeys Search Window screen.

4 Securing Email

This chapter explains how to secure email messages you send to others and decrypt and verify the messages others send to you.

Sending email that is not encrypted is like sending a postcard: the message you write can easily be read by someone in between you and the recipient.

To secure your email, PGP offers plug-ins that work along with your email applications and other utilities to encrypt, sign, decrypt, and verify email text. The PGP email plug-ins are available for seamless integration with Microsoft Exchange, Outlook and Express, Lotus Notes, Novell GroupWise, and QUALCOMM Eudora.

Encrypting and signing email

The quickest and easiest way to secure email communications is by using an email application supported by the PGP plug-ins. If you are using an email application that is not supported by the PGP plug-ins, you can encrypt, sign, decrypt and verify the text of your email messages using PGPtray icon.

Encrypting and signing email using the PGP plug-ins

Although the procedure varies slightly between different email applications, you perform the encryption and signing process by clicking the appropriate buttons in the application's toolbar.

To encrypt and sign with supported email applications:

1. Use your email application to compose your email message as you normally would.

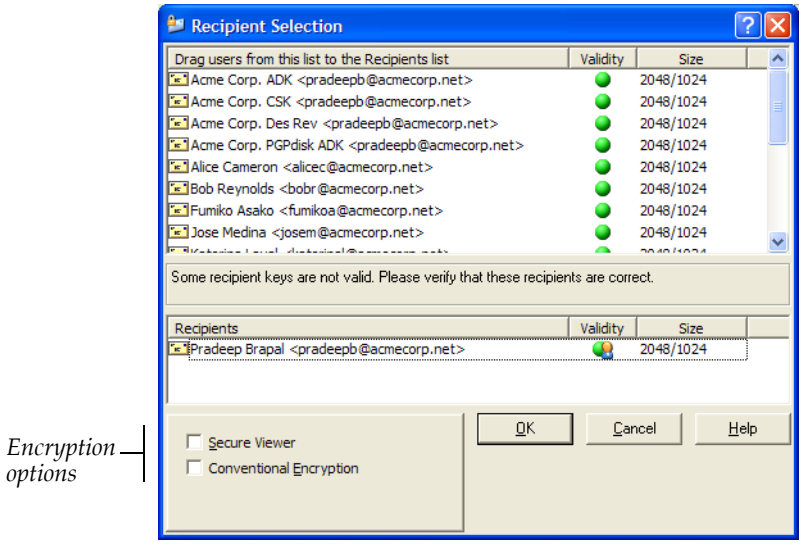
Note: If you are sending sensitive email, consider leaving your subject line blank or creating a subject line that does **not** reveal the contents of your encrypted message.

2. When you have finished composing the text of your email message, click the envelope and lock icon ( ) to encrypt the text of your message, then click the paper and pen icon ( ) to sign your message.
3. Send your message as you normally do.

   If you have a copy of the public keys for every one of the recipients, the appropriate keys are automatically used and the message is sent.

However, if you specify a recipient for whom there is no corresponding public key or one or more of the keys have insufficient validity, the PGP Recipient Selection screen appears so that you can specify the correct key.

You can force the PGP Recipient Selection screen to appear, even if you have a valid copy of the public keys for every one of the recipients, by holding down Shift when you click **Send**. You should do this if you want to use the Secure Viewer or Conventional Encrypt features and you do not want your message to be sent automatically.



4. Drag the public keys for those who are to receive a copy of the encrypted email message into the Recipients list box. You can also double-click any of the keys to move it from one area of the screen to the other.

   The Validity icon indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key.

5. You can choose from the following encryption options depending on the type of data you are encrypting:

   – **Secure Viewer.** Select this option to protect the data from TEMPEST attacks upon decryption. If you select this option, the decrypted data is displayed in a special TEMPEST attack prevention font that is unreadable to radiation capturing equipment, and cannot be saved in decrypted format. For more information about TEMPEST attacks, see the section on vulnerabilities in *An Introduction to Cryptography*.

Note: The Secure Viewer option may not be compatible with previous versions of PGP. Messages encrypted with this option enabled can be decrypted by previous versions of PGP; however, this feature may be ignored.

– **Conventional Encrypt.** Select this option to use a common passphrase instead of public key encryption. If you select this option, the message is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you will be asked to choose.

6. Click **OK** to encrypt and sign your mail.

   If you have elected to sign the encrypted data, the Signing Key Passphrase screen appears, requesting your passphrase before the mail is sent.

7. Enter your passphrase and then click **OK**.

Caution: If you do not send your email immediately but instead store it in your outbox, you should be aware that when using some email applications the information is not encrypted until the email is actually transmitted. Before queuing encrypted messages you should check to see if your application does in fact encrypt the messages in your outbox. If it does not, you can use PGPtray's Current Window option to encrypt your messages before queuing them in the outbox.

Encrypting and signing email without PGP plug-in support

If your email application does not support the PGP plug-ins, you can use PGPtray to encrypt the text of your message prior to sending it. The easiest way to encrypt your message without the use of a PGP plug-in is to use the **Current Window** options in PGPtray.

To encrypt and sign email without a PGP plug-in:

1. Use your email application to compose your email message as you normally would.

Note: If you are sending sensitive email, consider leaving your subject line blank or creating a subject line that does **not** reveal the contents of your encrypted message.

2. When you have finished composing the text of your email message, click on the PGPtray icon and select **Encrypt**, **Sign**, or **Encrypt & Sign** from the Current Window menu.
3. Select the public key of the recipient of the message and click **OK**.

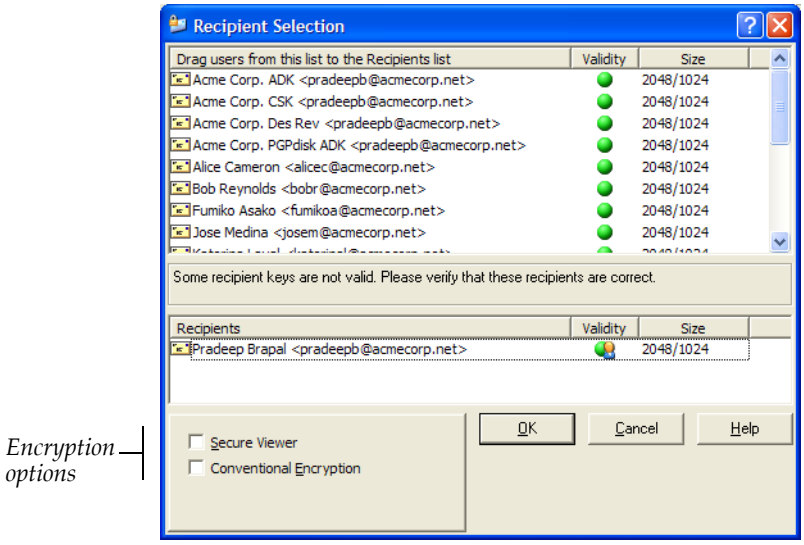
   Encrypted text appears in the email message window.

4. Send your message as you normally do.

   If you have a copy of the public keys for every one of the recipients, the appropriate keys are automatically used and the message is sent.

However, if you specify a recipient for whom there is no corresponding public key or one or more of the keys have insufficient validity, the PGP Recipient Selection screen appears so that you can specify the correct key.

You can force the PGP Recipient Selection screen to appear, even if you have a valid copy of the public keys for every one of the recipients, by holding down Shift when you click **Send**. You should do this if you want to use the Secure Viewer or Conventional Encrypt features and you do not want your message to be sent automatically.



5. Drag the public keys for those who are to receive a copy of the encrypted email message into the **Recipients** list box. You can also double-click any of the keys to move it from one area of the screen to the other.

   The Validity icon indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key.

6. You can choose from the following encryption options depending on the type of data you are encrypting:

   – **Secure Viewer.** Select this option to protect the data from TEMPEST attacks upon decryption. If you select this option, the decrypted data is displayed in a special TEMPEST attack prevention font that is unreadable to radiation capturing equipment, and cannot be saved in decrypted format. For more information about TEMPEST attacks, see the section on vulnerabilities in *An Introduction to Cryptography*.

Note: The Secure Viewer option may not be compatible with previous versions of PGP. Messages encrypted with this option enabled can be decrypted by previous versions of PGP; however, this feature may be ignored.

– **Conventional Encrypt.** Select this option to use a common passphrase instead of public key encryption. If you select this option, the message is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you will be asked to choose.

7. Click **OK** to encrypt and sign your mail.

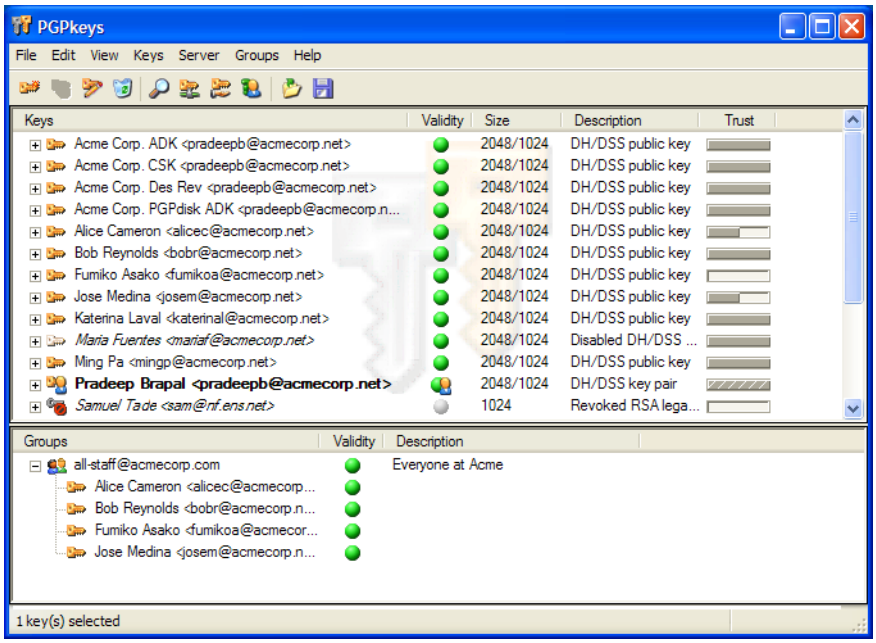
   If you have elected to sign the encrypted data, the Signing Key Passphrase screen appears, requesting your passphrase before the mail is sent.

8. Enter your passphrase and then click **OK**.

Caution: If you do not send your email immediately but instead store it in your outbox, you should be aware that when using some email applications the information is not encrypted until the email is actually transmitted. Before queuing encrypted messages you should check to see if your application does in fact encrypt the messages in your outbox. If it does not, you can use PGPtray's Current Window option to encrypt your messages before queuing them in the outbox.

Encrypting email to groups of recipients

You can use PGP to create group distribution lists. For example, if you want to send encrypted mail to 10 people at usergroup@pgp.com, you could create a distribution list with that name. The Groups menu in PGPkeys contains the Show Groups option that toggles the display of the Groups window in PGPkeys.



Note: If you intend to encrypt information to all members of an existing email distribution list, you must create a PGP group by the same name as, and including the same members as, the email distribution list. For example, if there is a *usergroup@pgp.com* list set up in your email application, you must create a usergroup@pgp.com group in PGP.

Working with distribution lists

Use the Groups feature to create distribution lists and to edit the list of people to whom you want to send encrypted email.

To create a group (distribution list):

1. Choose **New Group** from the **Groups** menu.
2. Enter a name for the group distribution list. Optionally, enter a group description. For example, you can name the group "everyone@pgp.com" with a description of "All employees."
3. Click **OK** to create the distribution list.

The group distribution list is added to your keyring and can be viewed in the Groups window.

To add members to a distribution list:

1. In the PGPkeys window, select the users or lists you want to add to your distribution list.
2. Drag the users from the PGPkeys window to the desired distribution list in the Groups window.

Note: Members in a distribution list can be added to other distribution lists.

To add a distribution list to another distribution list:

1. Select the distribution list that you want to add to another list.
2. Drag the selected list into the list to which it will be added.

To delete members from a distribution list:

1. Within the distribution list, select the member to be deleted.
2. Press **Delete**.

   PGP asks you to confirm your choice.

To delete a distribution list:

1. Select the distribution list to be deleted from the Groups window.
2. Press **Delete**.

Sending encrypted and signed email to distribution lists

To send encrypted and signed email to a distribution list:

1. Address the mail to your mail distribution list.

   The name of your encryption distribution list must correspond to the name of the email distribution list.
2. Use your email application to compose your email message just as you normally would.
3. When you have finished composing the text of your email message, click on the PGPtray icon and select **Encrypt**, **Sign**, or **Encrypt & Sign** from the Current Window menu.

   The PGP Key Recipients screen appears.
4. Select the recipient's public keys for the text you are encrypting or signing.

5. Send the message.

Decrypting and verifying email

The quickest and easiest way to secure email communications is by using an email application supported by the PGP plug-ins. If you are using an email application that is not supported by the PGP plug-ins, you can encrypt, sign, decrypt and verify the text of your email messages by using PGPtray.

Decrypting and verifying email using the PGP plug-ins

Although the procedure varies slightly between different email applications, when you are using an email application supported by the plug-ins, you can perform the decryption and verification operations by clicking the envelope icon in the message or your application's toolbar. In some cases you may need to select Decrypt/Verify from the menu in your email application. In addition, if you are using an application that supports the PGP/MIME standard, you can decrypt and verify your email messages as well as any file attachments by clicking an icon attached to your message.

If you are using an email application that is not supported by the PGP plug-ins, you will decrypt and verify your email messages via PGPtray. In addition, if your email includes encrypted file attachments, you must decrypt them separately via PGPtray.

To decrypt and verify from supported email applications:

1. Open your email message just as you normally do.

   You will see a block of unintelligible ciphertext in the body of your email message.

2. To decrypt and verify the message, click the locked envelope icon ( ).

   To decrypt and verify attached files, decrypt them separately using the PGPtray icon.

   The PGP Enter Passphrase screen appears, asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The message is decrypted. If it has been signed and you have the sender's public key, a message appears indicating whether the signature is valid.

   If the message is encrypted with the Secure Viewer option enabled, an advisory message appears. Click **OK** to continue. The decrypted message appears on a secure PGP screen in a special TEMPEST attack prevention font.

4. You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

Note: Messages encrypted with the Secure Viewer option enabled cannot be saved in their decrypted state.

Decrypting and verifying email without PGP plug-in support

If your email application does not support the PGP plug-ins, you can use PGPtray to decrypt the text of your message prior to sending it.The easiest way to decrypt your message without the use of a PGP plug-in is to use the Current Window options in PGPtray.

To decrypt and verify from non-supported email applications:

1. Open your email message just as you normally do.

   You will see a block of unintelligible ciphertext in the body of your email message.

2. In PGPtray, select **Current Window—>Decrypt/Verify**.

   If the email message includes encrypted file attachments, decrypt them separately with PGPtools or PGPtray.

   The PGP Enter Passphrase screen appears asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The message is decrypted. If it has been signed, a message appears indicating whether the signature is valid.

   If the message is encrypted with Secure Viewer enabled, an advisory message appears. Click **OK** to continue. The decrypted message appears on a secure PGP screen in a special TEMPEST attack prevention font.

4. You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

Note: Messages encrypted with the Secure Viewer option enabled cannot be saved in their decrypted state.

PGP/MIME

If you are using an email application with one of the plug-ins that supports the PGP/MIME standard, and you are communicating with another user whose email application also supports this standard, both of you can automatically encrypt and decrypt your email messages and any attached files when you send or retrieve your email. All you have to do is turn on the PGP/MIME encryption and sign functions from the Email tab of the PGP Options screen, which can be opened from PGPtray or from within PGPkeys.

When you receive email from someone who uses the PGP/MIME feature, the mail arrives with an icon in the message window indicating that it is PGP/MIME encoded.

To decrypt the text and file attachments in PGP/MIME encapsulated email and to verify any digital signatures, simply click the lock and quill icon. Attachments are still encrypted if PGP/MIME is not used, but the decryption process is usually more involved for the recipient.

When you encrypt and sign with an email application that is supported by the PGP plug-ins, you have two choices, depending on what type of email application the recipient is using. If you are communicating with other PGP users who have an email application that supports the PGP/MIME standard, you can take advantage of a PGP/MIME feature to encrypt and sign your email messages and any file attachments automatically when you send them. If you are communicating with someone who does not have a PGP/MIME-compliant email application, you should encrypt your email with PGP/MIME turned off to avoid any compatibility problems.

Refer to the following table for a list of plug-ins and their features.

	Eudora	Outlook	Outlook Express	Lotus Notes	Novell GroupWise
PGP/MIME	Yes	No	No	No	No
Auto-decrypt	No	Yes	Yes	Yes	Yes
Encrypt HTML	Yes	Yes	No	Yes	No
Preserve text formatting	Yes	Yes	No	Yes	No
Encrypt attachments	Yes	Yes	No	Yes	Yes
Encrypt/Sign defaults	Yes	Yes	Yes	Yes	Yes
Print decrypted email	Yes	Yes	No	Yes	No

5 Securing Files

This chapter describes how to use PGP to securely maintain files. It describes how to use PGP to encrypt, decrypt, sign, and verify files either for email or for secure storage on your computer. It also describes the PGP Wipe and Free Space Wipe functions, which delete files by erasing their contents completely from your computer.

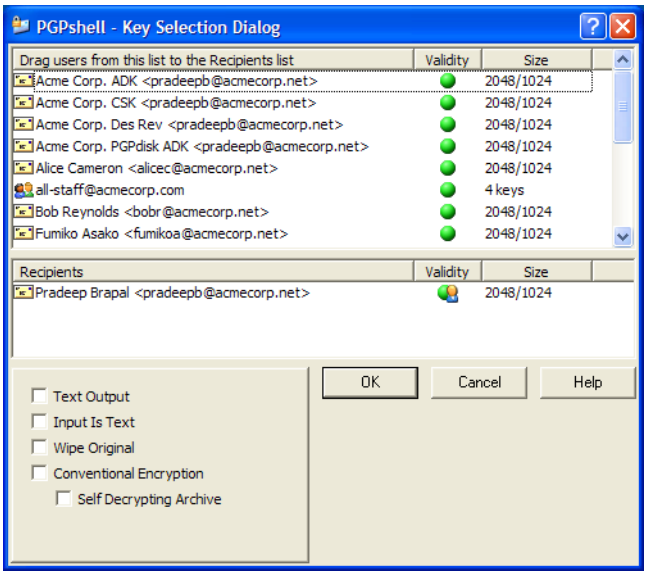
Securing your files and folders with PGP

You can use PGP to encrypt and sign files to use as email attachments as well as decrypt and verify files or attachments that have been encrypted to you.

Encrypting and signing files

Use the Encrypt, Sign, or Encrypt and Sign options available from PGPtray or the Windows Explorer File menu to secure your files and folders.

When you select Encrypt or Encrypt and Sign, the PGP Key Selection screen automatically appears; you use it to select the public keys of the recipients for the data you are encrypting.



Encryption options

You select the public keys by dragging them to the Recipients list. You can choose additional encryption options from the lower left menu. The options available to you depend upon the type of data that you are encrypting.

The options are:

- **Text Output.** When sending files as attachments with some email applications, you may need to select the **Text Output** check box to save the file as ASCII text. This is sometimes necessary in order to send a binary file using older email applications. Selecting this option increases the size of the encrypted file by about 30 percent.
- **Wipe Original.** Select this check box to overwrite the original document that you are encrypting, so that your sensitive information is not readable by anyone who can access your hard disk.
- **Secure Viewer.** Select this check box to protect text from TEMPEST attacks upon decryption. If you select this option, the data is displayed in a special TEMPEST attack prevention font that is unreadable to radiation capturing equipment upon decrypting, and your email can't be saved in decrypted format. For more information about TEMPEST attacks, see the vulnerabilities section in *An Introduction to Cryptography*. This option is only available when encrypting text or text files.
- **Conventional Encrypt.** Select this check box to rely on a common passphrase rather than on public key cryptography. The file is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you are asked to choose.
- **Self Decrypting Archive (SDA).** Select this check box to create a self decrypting executable file. If you select this option, the file is encrypted using a session key, which encrypts (and decrypts) using a passphrase that you are asked to choose, and PGP automatically appends an .sda.exe extension. The resulting executable file can be decrypted by simply double-clicking on it and entering the appropriate passphrase. This option is especially convenient for users who are sending encrypted files to people who do not have PGP software installed. Note that sender and recipient must be on the same operating system. Refer to Chapter 7, Self-Decrypting Archives for more information about SDAs.

If you are signing the files, you are asked to supply your passphrase. After encryption, if you look in the folder where the original file was located, you will find a file with the specified name represented by one of three icons:

encrypted with text output *encrypted with standard output* *self-decrypting archive output*

If you are encrypting or signing a folder, the output may be in a new folder, depending on the options you selected.

Decrypting and verifying files

When someone sends you encrypted data in a file, you can unscramble the contents and verify any appended signature to make sure that the data originated with the alleged sender and that it has not been altered.

Use the **Decrypt & Verify** option available from PGPtray or the Windows Explorer File to decrypt your files and folders.

To decrypt and/or verify data that has been encrypted to your key, you must have your private key and passphrase to complete the task. If the file was encrypted with the **Secure Viewer** option enabled, the decrypted text appears on a secure PGP screen in a special TEMPEST attack prevention font. Otherwise, the message will appear in its original state.

Note: Messages encrypted with the **Secure Viewer** option enabled cannot be saved in their decrypted state. They are only viewable on the secure PGP screen after decryption.

Signing and decrypting files with a split key

Whenever you want to sign or decrypt files with a split key, you must rejoin the key before you can perform the signing or decrypting task. See "Rejoining split keys" on page 138 for more information.

Permanently erasing files and free disk space

As you create and delete sensitive files on your computer, fragments from the data contained in the files remain in the free disk space of your computer. When you delete a file normally by placing it in the Recycle Bin, the name of the file is removed from the file directory but the data in the file remains on the disk. Even when you empty the Recycle Bin the data is not completely erased until the operating system overwrites the free disk space. Also, many programs create temporary files while you edit the contents of your documents. These files are deleted when you close the documents but your data is also left behind in free disk space.

In essence, your sensitive files are never completely erased and with the proper tools someone could retrieve your previously deleted files and even gather personal information from the free disk space of your computer.

If you want to completely destroy your sensitive files without leaving fragments of their data behind, use the PGP Wipe utility. When you delete a file using Wipe, the file is immediately overwritten (even on systems with virtual memory) and all traces of the file are removed so that it cannot be retrieved even by using disk recovery software.

In addition, you can set file wiping options from the General tab of the PGP Options screen. You can enable Wipe to automatically wipe files when deleting them. To learn how to set wiping options, see "Setting General options" on page 145.

To erase the free disk space that contains data from previously deleted files and programs, use PGP Free Space Wiper. To ensure that your deleted data is irrecoverable, erase your free disk space periodically with the Free Space Wiper.

Using PGP Wipe to permanently delete a file

Use the **Wipe** feature available from the PGPmail screen and the Windows Explorer File menu to permanently erase your files and folders.

To permanently delete your files and folders:

1. Right-click on the file and then choose **Wipe** from the menu, or drag the file onto the **Wipe** button ( ) on the PGPmail screen.

   A confirmation dialog box appears.

2. Click **OK** to permanently erase the file.

   To stop wiping the file before the task is completed, click **Cancel**.

   Clicking **Cancel** during file wipe can leave remnants of the file behind.

Caution: Many programs automatically save files in progress, so back-up copies of the file you deleted may exist. PGP Corporation recommends that you run the Wipe utility on the back-up copies as well as the original file to thoroughly erase it from your hard disk.

Using the Wipe Free Space Wizard to clean free disk space

Use the Wipe Free Space Wizard available from the PGPmail screen to clean your free disk space.

To wipe free space on your disks:

1. On the PGPmail screen, click the **Freespace Wipe** button ( ) to start the Freespace Wipe Wizard.

   The Wipe Free Space Wizard appears.

2. Read the information in the welcome screen, then click **Next** to advance to the next dialog box.

   The PGP Free Space Wipe Wizard prompts you to select the volume you want to wipe and the number of passes you want to perform.

3. In the **Volume** box, select the disk or volume that you want PGP to wipe. Then, select the number of passes that you want PGP to perform. The recommended guidelines are:
   - 3 passes for personal use
   - 10 passes for commercial use
   - 18 passes for military use
   - 26 passes for maximum security

Note: Commercial data recovery companies have been known to recover data that has been over written up to 9 times. PGP uses highly sophisticated patterns during each wipe to ensure that your sensitive data cannot be recovered.

4. Click **Next** to continue.

   The **Perform Wipe** dialog box opens and displays statistical information about the drive or volume you selected.

5. Click the **Begin Wipe** button to start freespace wiping your disk or volume.

   The PGP Free Space Wiper scans and then wipes leftover fragments from your disk or volume.

6. When the wipe session ends, click **Finish**.

Caution: Clicking **Cancel** during file wipe can leave remains of the file on your computer.

Scheduling folder and free space wiping

You can use the Windows Task Scheduler to schedule periodic folder and free space wiping for selected folders.

Note: To use this scheduling feature, you must have the Windows Task Scheduler installed on your system. If you do not have the Task Scheduler installed on your system, you can download it from the Microsoft Web site (http://www.microsoft.com).

To schedule folder and free space wiping:

1. On the PGPmail screen, click the **Freespace Wipe** button ( ) to start the Freespace Wipe Wizard.

   The **Wipe Free Space Wizard** appears.

2. Read the information in the welcome screen, then click **Next** to advance to the next dialog box.

   The PGP Free Space Wipe Wizard prompts you to select the volume you want to wipe and the number of passes you want to perform.

3. In the Volume box, select the disk or volume that you want PGP to wipe. Then, select the number of passes that you want PGP to perform. The recommended guidelines are:

   – 3 passes for personal use

   – 10 passes for commercial use

   – 18 passes for military use

   – 26 passes for maximum security

Note: Commercial data recovery companies have been known to recover data that has been over written up to nine times. PGP uses highly sophisticated patterns during each wipe to ensure that your sensitive data cannot be recovered.

4. Click **Next** to continue.

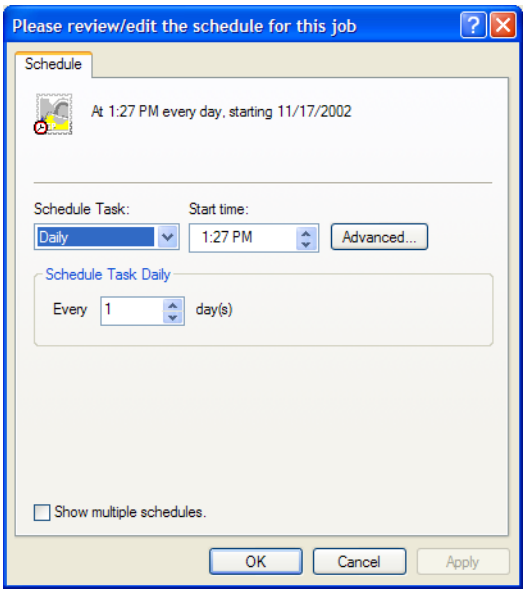
5. When the Perform Wipe screen opens, click the **Schedule** button.

6. When the Schedule screen appears, click **OK** to continue.

   If you are running Windows NT, the Windows NT Confirm Password dialog box appears.

   Enter your Windows NT login password in the first text box. Press **Tab** to advance to the next text box and confirm your entry by entering your password again. Click **OK**.

The Windows Task Schedule screen appears.



7. Choose how often you want the task to run from the Schedule Task area. Your choices are:
   - **Daily.** This option runs your task once at the time you specify on the days you indicate. Click **OK** to close the dialog box, then enter the time you want to run the task each day in the Start Time text box.
   - **Weekly.** This option runs your task on a weekly basis at the date and time you specify. Enter the number of weeks you want between each disk wipe in the text box provided, then choose a day from the Schedule Task Weekly list.
   - **Monthly.** This option runs your task once each month on the day and at the time you specify. Enter the time in the text box provided, then enter the day of the month on which you want the task to run. Click **Select Months** to specify which months the task will run.
   - **Once.** This option runs your task exactly once on the date and at the time you specify. Enter the time in the text box provided, then select a month and a date from the lists Run On text box.
   - **At System Start up.** This option runs your task only upon system start up.
   - **At Logon.** This option runs your task when you log on to your computer.
   - **When Idle.** This option runs your task when your system is idle for the amount of time you specify in the minutes text box.
8. Enter the time of day that you want the task to start in the Start Time box.
9. Specify how often you want the task to run in the Schedule Task Daily box.

10. Click **Advanced** to open a dialog box where you can select additional scheduling options, such as the start date, the end date, and the duration of the task.
11. Click **OK**.

    A confirmation dialog box appears. Your new PGP folder or free space task is now scheduled. To edit or delete your PGP tasks, use the Windows Task Scheduler.

6 Wiping

This chapter tells you how PGP can wipe files and free disk space on your systems so that sensitive data cannot be retrieved, even using disk recovery software. It also tells you how you can schedule automatic free space wiping.

Overview

If you want to completely destroy sensitive files without leaving fragments of their data behind, use the PGP Wipe utility. When you delete a file using Wipe, the file is immediately overwritten (even on systems with virtual memory) and all traces of the file are removed so that it cannot be retrieved even by using disk recovery software.

In addition, you can set file wiping options from the General tab of the PGP Options screen. You can enable Wipe to automatically wipe files when deleting them. To learn how to set wipe options, see "Setting General options" on page 145.

To erase free disk space that could contain data from previously deleted files and programs, use the PGP Free Space Wiper utility. To make sure your deleted data is not recoverable, erase your free disk space periodically with the Free Space Wiper.

It is especially important to use the Free Space Wiper on Journaling filesystems such as NTFS, as such filesystems make a second copy of everything written to disk in a filesystem journal. This helps the disk recover from damage, but requires extra work when removing sensitive data. Wiping a file does not wipe any potential journal entries that may have been created. NTFS in particular can also store small (less than 1K) files in internal data structures that cannot be wiped properly without using the PGP Free Space Wiper with the "Wipe NTFS internal data structures" option.

Depending on the number of passes you select, PGP's wiping utilities can greatly exceed U.S. government and military recommendations for secure data erasure.

Using PGP Wipe to permanently delete a file

Use the PGP Wipe utility to permanently erase sensitive files and folders.

To permanently erase sensitive files and folders:

1. Right-click on the file, slide down to **PGP**, then over to **Wipe** from the menu, or drag the file over the **Wipe** button on the PGPmail screen.

   A wipe confirmation screen appears.

2. Click **Yes** to permanently erase the file.

   To stop wiping the file before the task is completed, click **No**.

Clicking **Cancel** during the wiping of a file can leave remnants of the file behind.

Caution: Many programs automatically save files in progress, so backup copies of the file you deleted may exist. PGP Corporation recommends that you run the Wipe utility on the backup copies as well as the original file to thoroughly erase it from your system. The best way to handle this situation is to enable PGP's "Automatically wipe on delete" option on the General Options tab (see "Setting General options" on page 145).

Using the Wipe Free Space Wizard to clean free disk space

Use the PGP Wipe Free Space Wizard to clean your free disk space.

To wipe free space on your disks:

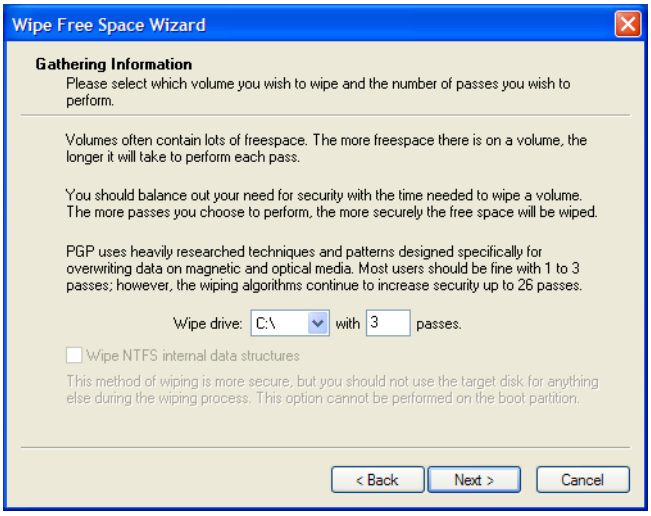
1. On the PGPmail screen, click the **Freespace Wipe** button.

   The Welcome screen of the Wipe Free Space Wizard appears.

Wipe Free Space Wizard
Welcome to the PGP Wipe Free Space Wizard
When a file is deleted by your computer, the data that was in the file actually remains on your hard drive. Over time, this leads to a large amount of potentially sensitive data left behind in random places on your drive.
Using PGP's file wiping feature when you delete files solves only part of the problem because many files are created and deleted by applications or operating system without your knowledge.
PGP's volume wiping cleans all the free space on your hard drive which does not contain actual file data including all deleted files, their directory entries, and the little areas after the end of existing files which may still have old data left behind.
PGP
< Back
Next >
Cancel

2. Read the information, then click **Next**.

The Gathering Information screen appears.


Wipe Free Space Wizard
Gathering Information
Please select which volume you wish to wipe and the number of passes you wish to perform.
Volumes often contain lots of freespace. The more freespace there is on a volume, the longer it will take to perform each pass.
You should balance out your need for security with the time needed to wipe a volume. The more passes you choose to perform, the more securely the free space will be wiped.
PGP uses heavily researched techniques and patterns designed specifically for overwriting data on magnetic and optical media. Most users should be fine with 1 to 3 passes; however, the wiping algorithms continue to increase security up to 26 passes.
Wipe drive: C:\ with 3 passes.
Wipe NTFS internal data structures
This method of wiping is more secure, but you should not use the target disk for anything else during the wiping process. This option cannot be performed on the boot partition.
< Back
Next >
Cancel

3. In the Wipe Drive box, select the disk or volume you want PGP to wipe and the number of passes you want PGP to perform. The recommended guidelines are:
   - 3 passes for personal use
   - 10 passes for commercial use
   - 18 passes for military use
   - 26 passes for maximum security

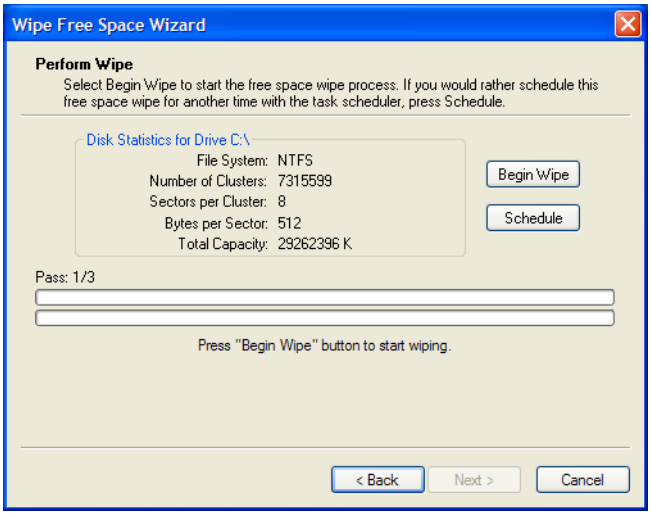
Note: Commercial data recovery companies have been known to recover data that has been overwritten up to nine times. PGP uses highly sophisticated patterns during each wipe to make sure your sensitive data cannot be recovered.

4. Choose whether to wipe internal NTFS data structures.

   If the selected partition is *not* your boot partition, you may perform an intensive wipe operation that overwrites internal NTFS data structures that may hold residual data. The partition will be completely filled during this process, and as such youshould not use the disk for anything else while this operation is in progress. Some of these structures are not generally considered free space on your drive, but the techniques employed by this option will cause them to be wiped. This option does not increase the risk of anything negative happening to your disk as a result of the wiping operation.

5. Click **Next**.

The Perform Wipe screen opens and displays statistical information about the drive or volume you selected.


Wipe Free Space Wizard
Perform Wipe
Select Begin Wipe to start the free space wipe process. If you would rather schedule this free space wipe for another time with the task scheduler, press Schedule.
Disk Statistics for Drive C:\
File System: NTFS
Number of Clusters: 7315599
Sectors per Cluster: 8
Bytes per Sector: 512
Total Capacity: 29262396 K
Begin Wipe
Schedule
Pass: 1/3
Press "Begin Wipe" button to start wiping.
< Back
Next >
Cancel

6. Click **Begin Wipe**.

   The PGP Free Space Wiper scans and then wipes leftover fragments from your disk or volume.

   When the wipe session is complete, a message appears near the bottom of the Perform Wipe screen telling you the selected drive has been wiped.

7. Click **Next**.

   The Completing screen appears.

Wipe Free Space Wizard
Completing the PGP Wipe Free Space Wizard
Congratulations!
You have successfully free space wiped your disk drive. Data that has been previously erased will be unrecoverable.
Click Finish to close this Wizard.
PGP
< Back
Finish
Cancel

8. Click **Finish**.

Scheduling folder and free space wiping

You can use the Windows Task Scheduler to schedule periodic folder and free space wiping.

Note: To use this scheduling feature, you must have the Windows Task Scheduler installed on your system. If you do not have the Task Scheduler installed on your system, you can download it from the Microsoft Web site (www.microsoft.com).

To schedule folder and free space wiping:

1. On the PGPmail screen, click the **Freespace Wipe** button to start the Freespace Wipe Wizard.

   The Wipe Free Space Wizard appears.

2. Read the information on the Welcome screen, then click **Next** to continue.

   The PGP Free Space Wipe Wizard prompts you to select the volume you want to wipe and the number of passes you want to perform.

3. In the Volume box, select the disk or volume that you want PGP to wipe. Then, select the number of passes that you want PGP to perform. The recommended guidelines are:

   – 3 passes for personal use

   – 10 passes for commercial use

   – 18 passes for military use

   – 26 passes for maximum security

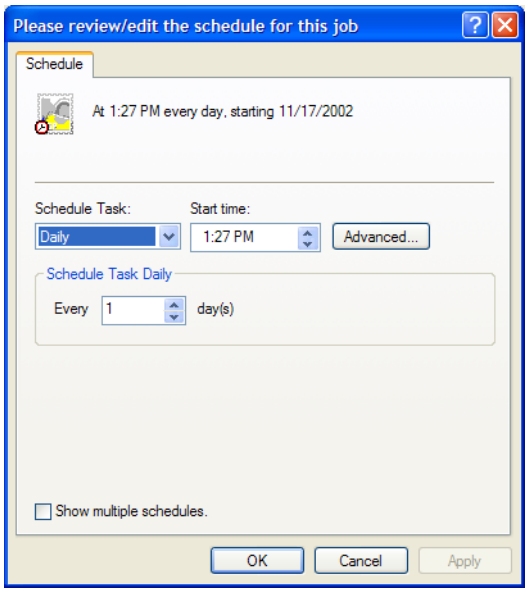
Note: Commercial data recovery companies have been known to recover data that has been over written up to nine times. PGP uses highly sophisticated patterns during each wipe to ensure that your sensitive data cannot be recovered.

4. Click **Next** to continue.
5. When the Perform Wipe screen opens, click the **Schedule** button.
6. When the Schedule screen appears, click **OK** to continue.

   If you are running Windows NT, the Windows NT Confirm Password dialog box appears.

   Enter your Windows NT login password in the first text box. Press **Tab** to advance to the next text box and confirm your entry by entering your password again. Click **OK**.

The Windows Task Schedule screen appears.



7. Choose how often you want the task to run from the Schedule Task area. Your choices are:
   - **Daily.** This option runs your task once at the time you specify on the days you indicate. Click **OK** to close the dialog box, then enter the time you want to run the task each day in the Start Time text box.
   - **Weekly.** This option runs your task on a weekly basis at the date and time you specify. Enter the number of weeks you want between each disk wipe in the text box provided, then choose a day from the Schedule Task Weekly list.
   - **Monthly.** This option runs your task once each month on the day and at the time you specify. Enter the time in the text box provided, then enter the day of the month on which you want the task to run. Click **Select Months** to specify which months the task will run.
   - **Once.** This option runs your task exactly once on the date and at the time you specify. Enter the time in the text box provided, then select a month and a date from the lists Run On text box.
   - **At System Start up.** This option runs your task only upon system start up.
   - **At Logon.** This option runs your task when you log on to your computer.
   - **When Idle.** This option runs your task when your system is idle for the amount of time you specify in the minutes text box.
8. Enter the time of day that you want the task to start in the Start Time box.
9. Specify how often you want the task to run in the Schedule Task Daily box.

10. Click **Advanced** to open a dialog box where you can select additional scheduling options, such as the start date, the end date, and the duration of the task.
11. Click **OK**.

    A confirmation screen appears.

    Your new PGP folder or free space task is now scheduled. To edit or delete your PGP tasks, use the Windows Task Scheduler.

7 Self-Decrypting Archives

A self-decrypting archive (SDA) is a self-decrypting executable file that is conventionally encrypted using a passphrase you specify. The resulting file can be decrypted simply by double clicking it and entering the correct passphrase.

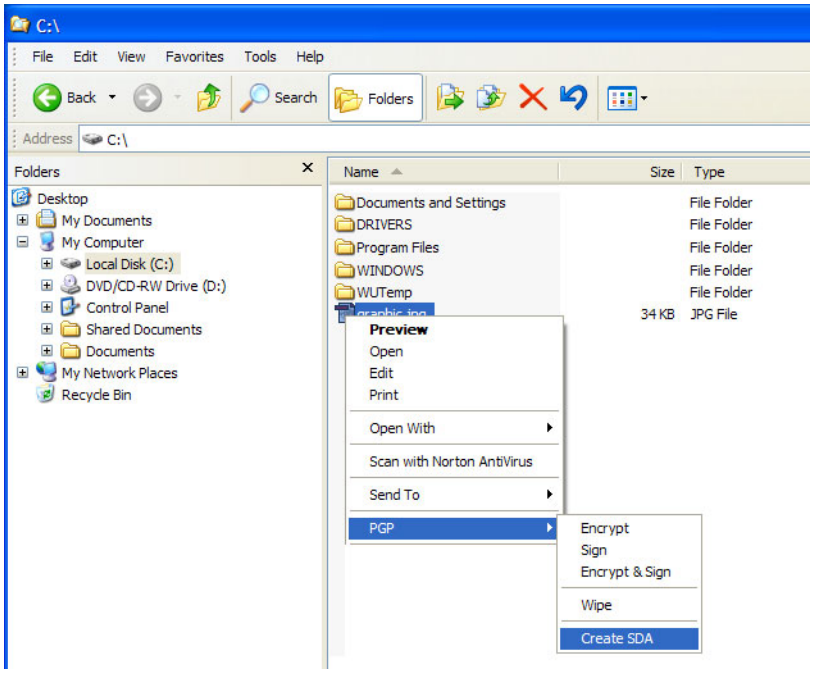
SDAs are valuable for situations where you need to send encrypted data to someone who doesn't have PGP. SDAs can be a single file, multiple files, a directory, multiple directories, or even an entire drive. All SDAs use the CAST5 algorithm.

Note: SDAs can only be opened under the same operating system as they were created under. In other words, you can't open an SDA on a Macintosh if it was created by the Windows version of PGP, and vice versa.

Creating an SDA

To create an SDA:

1. Select the files, directories, or drive you want to include in the SDA.
2. Right-click on your selection, slide down to **PGP**, then over and down to **Create SDA**.



The Enter Passphrase screen appears.

3. Enter the passphrase you want to use for this SDA, then enter it again for confirmation.

Note: You must be able to securely communicate this passphrase to the person who is going to be decrypting the SDA.

4. If you're creating an SDA with a file or files specifically selected (that is, not on the drive or in a directory, but specifically selected), you'll be prompted to confirm the filename and location of the SDA.

   If no file is specifically selected, you won't be prompted for a filename or location.

5. Click **Save**.

   PGP creates the SDA with contents you specified.

   The default filename for an SDA with a file or files specifically selected is the name of one of the files in the SDA with **.sda.exe** appended. The default filename for an SDA with no files specifically selected (that is, just directories or drives) is the name of one of the directories or drives with **.sda.exe** appended.

   Unless you specified otherwise, the SDA is saved in the same location as the original files.

Opening an SDA

To open an SDA:

1. Double click the SDA file. (It should have an extension of .sda.exe.)

   The PGP Self Decrypting Archive - Enter Passphrase screen appears.

2. Enter the appropriate passphrase and specify a location for the files in the SDA to be decrypted to, then click **OK**.

   The SDA is decrypted.

Note: If you are decrypting the SDA in the same location as where you got the files that are in the SDA, you'll be prompted to save the files to a different location or with a different name, so as not to overwrite the original files.

8 Securing ICQ

This chapter describes how PGP can secure your ICQ communications.

About ICQ

ICQ ("I Seek You") is an Internet application that allows you to communicate with friends and colleagues over the Internet in real time. As with any type of communication, especially through Internet-based applications, your conversation is not secure and is subject to eavesdropping.

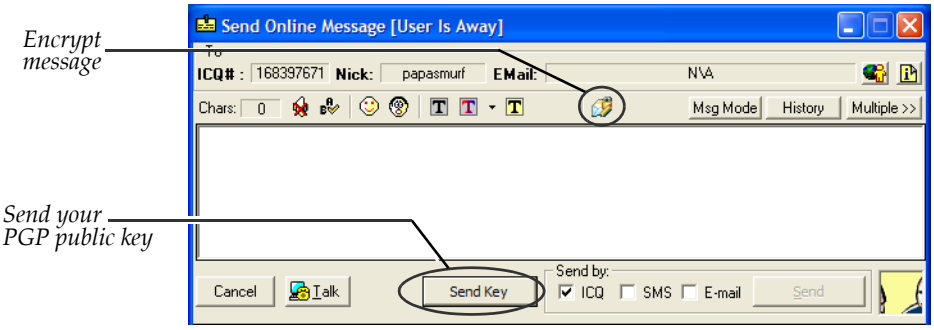
To secure your ICQ communications, PGP offers a powerful integrated plug-in that lets you easily encrypt and decrypt your ICQ messages and exchange PGP keys through ICQ.

Caution: ICQ allows you to send messages of unlimited length to online users. Offline users, however, are limited to receiving messages no longer than 450 characters. Because of this limitation and because the size of encrypted text can exceed the size of the original text, we recommend that you send your key and encrypted messages to online recipients only.

The PGP plug-in for ICQ allows you to secure your ICQ communications by encrypting your messages before you send them over the Internet, and decrypting and verifying automatically upon opening encrypted instant messages. Since the plug-in uses your PGP key together with your ICQ number to encrypt and secure your ICQ messages, it can automatically verify and decrypt the ICQ messages that are encrypted to your PGP key.

When the PGP plug-in for ICQ is installed on your system, the lock icon ( ) and the **Send Key** button appear in your **ICQ Send Online Message** dialog box.

Note: If you are using ICQ version 2000b or higher, then you must work in ICQ's **Advanced mode** (not Simple mode) and you must use the **Single Message mode window** (not the Split Message mode window) in order for the PGP plug-in buttons to appear.



Before you can encrypt an ICQ message, you must obtain the public key of the person for whom you are sending the encrypted message. You can obtain the recipients' public key and add it to your PGP keyring through ICQ.

Exchanging public keys in ICQ

To begin sending and receiving encrypted instant messages within ICQ, you must exchange public keys with each person with whom you want to securely correspond. With the PGP plug-in, you can send and receive PGP public keys through the ICQ application as well as send encrypted messages.

Sending your public key through ICQ

You can send your PGP public key to someone through ICQ. Your public key has your ICQ number attached to it.

To send your PGP public key to someone through ICQ:

1. Double-click on the name of the person in your ICQ Contact List to open the **ICQ Send Online Message** dialog box.
2. If you want to send a message along with your key, enter the message text just as you normally would.
3. Click the **Send Key** button.

   The first time you use PGP with ICQ, the **PGP ICQ Wizard** appears. Use the wizard to add your ICQ number as an identifier to your PGP key allowing others to send messages to you automatically. If the wizard appears, continue with instructions outlined in "Using the PGP ICQ Wizard" on page 57.

   Your PGP public key combined with your ICQ number is sent to the recipient.

Note: This text is **not** encrypted.

Using the PGP ICQ Wizard

Use the PGP ICQ wizard to add your ICQ number as an identifier to your PGP key. The wizard guides you through the process of selecting the key you want to use when securely communicating via ICQ and adding your ICQ number to the key.

To use the PGP ICQ Wizard:

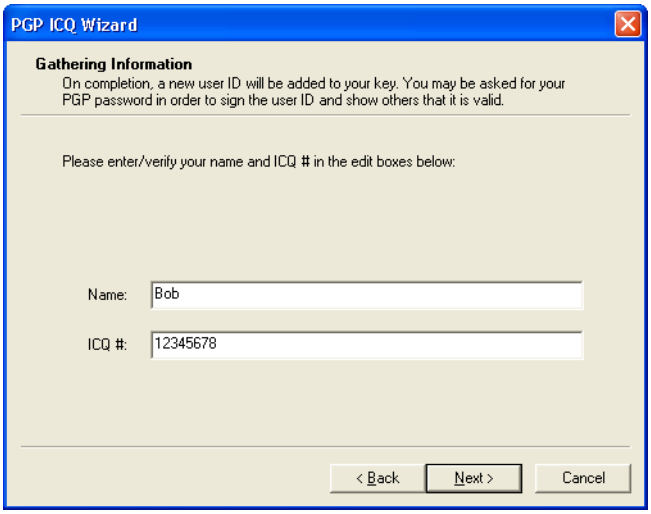
1. The PGP ICQ Wizard starts automatically when you click **Send** in ICQ but you don't have an ICQ number on your PGP key.

   The PGP ICQ Wizard Welcome screen appears.

PGP ICQ Wizard
Welcome to the PGP ICQ Wizard
An ICQ number could not be found on any of the valid user IDs for your default PGP key.
In order to allow others to send ICQ messages to you automatically, you should create a user ID on your key which contains your ICQ #.
This wizard will assist you in this process. Please press next to begin adding your ICQ # to your default PGP key.
PGP
< Back
Next >
Cancel

2. Read the information in the Welcome screen, then click **Next**.

   The PGP ICQ Wizard Gathering Information screen appears with your default user ID in the Name field and your ICQ number in the ICQ # field.


PGP ICQ Wizard
Gathering Information
On completion, a new user ID will be added to your key. You may be asked for your PGP password in order to sign the user ID and show others that it is valid.
Please enter/verify your name and ICQ # in the edit boxes below:
Name:
Bob
ICQ #:
12345678
< Back
Next >
Cancel

3. Make sure the user ID displayed in the Name field belongs to the key you want to use for securing your ICQ sessions. If you want to specify a different key, enter the key's user ID.
4. Click **Next**.

   The PGP Passphrase screen appears.
5. Enter your PGP passphrase, and then click **OK**.

   The PGP ICQ Wizard Completing screen appears.

PGP ICQ Wizard
Completing the PGP ICQ Wizard
Your ICQ # has been added to your PGP key. Users who communicate with you via ICQ will now be able to automatically send you encrypted messages.
If you are communicating for the first time with another ICQ user using PGP, you will want to send them your PGP key by pressing the Send Key button located at the bottom of the ICQ message composition window.
Enabling the Encrypt toolbar button located near the top of the ICQ message composition window will cause your message to be encrypted to the key of the recipient, providing you have their PGP key on your keyring.
PGP
< Back
Finish
Cancel

6. Click **Finish**.

   PGP adds your ICQ number to your key as a new user ID, and returns to the message you were sending.

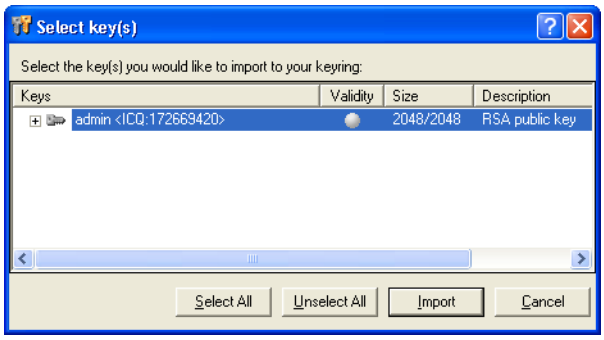
Adding a public key from ICQ to your keyring

When someone sends you a PGP public key through ICQ, you can add it to your keyring directly from the ICQ message.

To add a PGP public key to your keyring from an ICQ message:

1. Open the message that contains the PGP key.

   The sender's public key is displayed in the text field of the **Select Key(s)** screen.



2. Select the key, and then click **Import**.

   The key is imported to your PGP keyring.

   If your keyring already contained the public key for this user, then PGP adds the ICQ ID to the key. If you keyring did not already contain the public key for this user, then PGP adds the key to your keyring.

Encrypting ICQ messages

To send an encrypted ICQ message:

1. Exchange public keys with the person to whom you want to send secure messages.
2. Compose the message just as you normally would.

Note: Formatting in your ICQ message is lost when the message is decrypted.

3. When you are finished composing the message, click the lock icon ( ) that appears on your **ICQ Send Online Message** dialog box.

   The message text is encrypted.

4. Click **Send**.

9 Using Lotus Notes

This chapter tells you how to use PGP's Lotus Notes plugin.

The sections in this chapter are:

- Overview
- Encrypting and signing
- Decrypting and verifying

Overview

The PGP Lotus Notes plugin lets you encrypt, sign, and decrypt/verify encrypted email messages using your Lotus Notes email program.

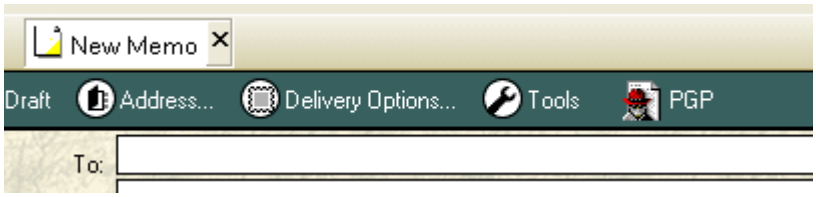
Encrypting and signing

To encrypt and sign an email message using Lotus Notes:

1. Use your Lotus Notes email client to compose your message as you normally would.

Note: If you are sending sensitive email, consider leaving your subject line blank or creating a subject line that does **not** reveal the contents of your encrypted message.

2. When you have finished composing the text of your email message, click the **PGP** button on your toolbar.



A drop-down menu appears listing your PGP options.

3. Select **Sign** to digitally sign your message; select **Encrypt** to encrypt the text of your message.
4. If you choose to encrypt and/or sign the message, you are also given the option to encrypt the text before sending. To do so, click the **PGP** button, and select **Encode NOW** from the new drop-down menu.

5. Send your message as you normally do.

   If you have a copy of the public keys for every one of the recipients on your keyring, and the recipients name or email address matches a user ID on your keyring, then the appropriate keys are used automatically.

   If the recipients name or email address does not match a user ID on your keyring, if there is no corresponding public key on your keyring for the recipient, or if one or more of the keys have insufficient validity, then the PGP Recipient Selection screen appears so that you can specify the correct key.

   You can force the PGP Recipient Selection screen to appear, even if you have a valid copy of the public keys for every one of the recipients, by holding down **Shift** when you click **Send**. You should do this if you want to use the Secure Viewer or Conventional Encrypt options and you do not want your message to be sent automatically.

6. Drag the public keys for those who are to receive a copy of the encrypted email message into the Recipients list box. You can also double-click any of the keys to move it from one area of the screen to the other.

   The Validity icon indicates the minimum level of confidence that the public keys in the Recipient list are valid. This validity is based on the signatures associated with the key.

7. You can choose to conventionally encrypt your email message. Select the **Conventional Encryption** check box to use a common passphrase instead of public key encryption. If you select this option, the message is encrypted using a session key, which encrypts (and decrypts) using a passphrase you will be asked to specify.

8. Click **OK** to encrypt and sign your mail.

   If you have elected to sign the encrypted data, the Signing Key Passphrase screen appears, requesting your passphrase before the mail is sent.

9. Enter your passphrase and then click **OK**.

Caution: If you do not send your email immediately but instead store it in your outbox, you should be aware that when using some email applications the information is not encrypted until the email is actually transmitted. Before queuing encrypted messages you should check to see if your application does in fact encrypt the messages in your outbox. If it does not, you can use PGPtray's **Current Window** option to encrypt your messages before queuing them in the outbox.

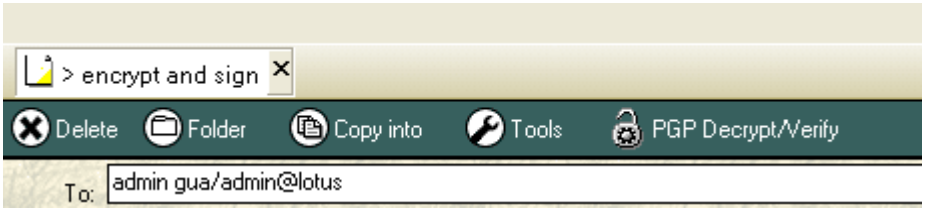
Decrypting and verifying

To decrypt and verify email using Lotus Notes:

1. Open your email message as you normally do.

   You will see a block of unintelligible ciphertext in the body of your email message.

2. To decrypt and verify the message, click the **PGP Decrypt/Verify** button on your toolbar.



   The PGP Enter Passphrase screen appears, asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The message is decrypted. If it has been signed and you have the sender's public key, the signature verification will appear in the PGP Log.

Note: You can save the message in its decrypted state, or you can save the original encrypted version so that it remains secure.

To decrypt and verify email attachments using Lotus Notes:

1. After decrypting the email message as instructed above, double-click on the attachment.

Note: You can also decrypt attachments without first decrypting the email message. Simply double-click on the attachment, click the **Launch** button, and enter your PGP passphrase when prompted.

2. Select **Launch**, then click **OK**.

   The PGP Enter Passphrase screen appears, asking you to enter your passphrase.

3. Enter your passphrase, then click **OK**.

   The attachment is decrypted.

Note: You can save the attachment in its decrypted state, or you can save the original encrypted version so that it remains secure.

10 Using Smart Cards

This chapter describes smart cards and tells you how to use them with PGP.

The sections in this chapter are:

- Overview
- Generating a keypair on a smart card
- Examining smart card properties
- Copying your public key from a smart card to someone's keyring
- Wiping keys from your smart card
- Copying a keypair from your keyring to a smart card

Overview

A smart card, sometimes called an intelligent token, is a portable device that includes a computer chip, which lets it store data and perform computations. Smart cards come in multiple form factors; they can be plastic cards about the size of a credit card or keychain fobs with USB connectors on one end, for example.

In order to use PGP with a smart card, you must have a supported smart card reader and the appropriate software drivers installed on your system. PGP Corporation strongly recommends using software drivers from the vendor who makes your smart card reader. They must include the PKCS-11 (the cryptographic token interface standard) library.

You can create and store your PGP keys on a smart card and access them using a PIN rather than a passphrase. The smart card has the added protection of being with you at all times—a key on a smart card is less vulnerable than the same key stored on your computer.

The private portion of your keypair that is generated on a smart card never leaves the smart card—it's not exportable. Decryption and signing operations take place directly on the card. The exception to this is if you generate a keypair on your desktop, rather than on the smart card, and then afterwards copy the keypair to your smart card.

Note: You ***must*** specify the smart card type in the Advanced tab of the PGP Options screen before you can generate a PGP keypair on a smart card. Refer to "Setting Advanced options" on page 155 for more information.

Generating a keypair on a smart card

Make sure to specify the appropriate smart card type in the Advanced tab of the PGP Options screen **before** you generate a PGP keypair on your smart card. If you don't, the smart card check box will not display.

To generate a PGP keypair on a smart card:

1. Put your smart card in the smart card reader.

Caution: Removing your smart card from the smart card reader while generating a keypair on the smart card may result in unpredictable behavior.

2. Open PGPkeys.
3. Click the **New Key** button on the PGPkeys menu bar.

   The Key Generation Wizard Welcome screen appears.
4. Click the **Expert** button.

   The Key Generation Wizard Expert panel appears.
5. Enter your name in the Full Name box and your email address in the Email Address box.

   It is not absolutely necessary to enter your real name or email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and others can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient.
6. In the Key Type box, select the type of key you want to create.

   Diffie-Hellman/DSS keys are ***not*** supported on smart cards.
7. In the Key Size box, select a key size of **1024** bits.
8. Indicate when you want your keys to expire. You can either use the default selection, **Never**, or you can enter a specific date after which the keys will expire.

   Once you create a keypair and have distributed your public key to the world, you will probably continue to use the same keys from that point on. However, under certain conditions you may want to create a special keypair that you plan to use for only a limited period of time. In this case, when the public key expires, it can no longer be used by someone to encrypt mail to you but it can still be used to verify your digital signature. Similarly, when your private key expires, it can still be used to decrypt mail that was sent to you before your public key expired but can no longer be used to sign mail to others.

9. Select the **Generate key on Smart Card** check box.

Note: The Generate key on Smart Card check box does not appear if the smart card is not inserted in the smart card reader or if you have not specified a smart card type on the Advanced tab of the PGP Options screen.

10. Click **Next**.
11. If PGP detects that your computer is in a Microsoft Exchange Server environment or if your PGP administrator has configured PGP to include specific installation settings, the Administrator Options panel appears. Read the information on this panel, then click **Next** to continue.
12. On the Passphrase panel, enter the PIN that corresponds to the smart card. The PIN acts as your PGP passphrase.

    Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the **Hide Typing** check box.
13. Click **Next** to begin the key generation process.

    PGP generates your new keypair directly on your smart card.

    This process can take several minutes.

    If you are in a Microsoft Exchange Server environment, PGP informs you that it needs to retrieve your email user ID from your Exchange server in order to add it to your new PGP key. If this is the case, continue with the instructions outlined in "Adding your email ID from your Microsoft Exchange Server to your new key" on page 102.
14. When the key generation process indicates that it is done, click **Next**.
15. Click **Finish**.

    Your new keypair is generated and stored directly on your smart card. Since the smart card is in the smart card reader, your key appears on your keyring and is represented by a key on a card icon ( ).

    Because the private portion of your keypair stays only on the smart card, when you remove the smart card from the smart card reader, the key icon changes to a single key to reflect that the public portion is left on the keyring and the private portion has been removed with the smart card.

Examining smart card properties

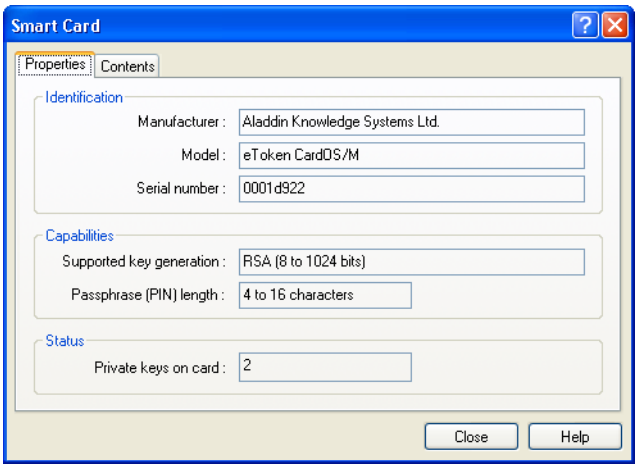
A key stored on a smart card is noted in the PGPkeys window with a special key and card icon ( ). By viewing the smart card properties, you can find information regarding the card itself, such as the manufacturer, serial number, and key types it supports, as well as view a list of the keys stored on the card.

To view smart card properties:

1. Open PGPkeys.
2. Put your smart card in your smart card reader.

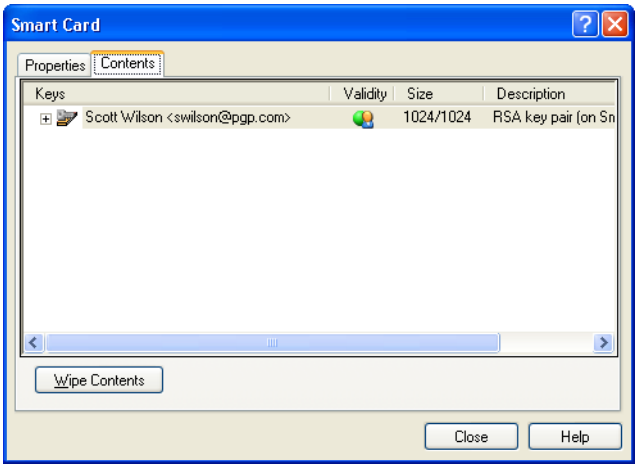
   A gold card icon ( ) appears in the lower left corner of the PGPkeys window.
3. Do one of the following:
   - Click the gold card icon found in the lower left corner of the PGPkeys window.
   - Pull down the View menu and select **Smart Card Properties**.

   The Smart Card window appears.



   The Properties tab displays information about the card, including:
   - the name of the manufacturer
   - the smart card model
   - the serial number associated with the smart card
   - its capabilities, including the type of PGP key that the card can store and the number of characters your PIN may contain
   - the total number of private keys you currently have on the smart card, including subkeys

4. To view a list of the keys stored on the smart card, or to wipe the contents of the smart card, click the **Contents** tab.



The Contents tab displays information about the PGP data stored on the smart card. Under Keys, a list of the keys stored on the smart card displays. You can find out more information about each key by viewing the signatures and user IDs associated with each key.

The **Wipe Contents** button enables you to completely erase all data stored on the smart card (see "Wiping keys from your smart card" on page 70 for more information).

Copying your public key from a smart card to someone's keyring

Storing your keys on a smart card enables you to physically walk to a computer—a computer with a compatible smart card reader and PGP installed, of course—and automatically copy the public portion of your keypair to a PGP keyring on that system.

To copy your public key from your smart card to another user's keyring:

1. Open PGPkeys.
2. Put your smart card into the smart card reader.
3. Wait for your key to display in PGPkeys.

   When you see your key display, it means that your public key has been copied onto the system.
4. Remove your smart card from the smart card reader.

   Your public key remains on the system.

Wiping keys from your smart card

You can delete all data stored on your smart card by using the Wipe Contents feature in the Smart Card properties window.

To wipe your smart card:

1. Open PGPkeys.
2. Put the smart card you want to wipe in the smart card reader.

   A gold card icon ( ) appears in the lower left corner of the PGPkeys window.

Caution: Removing your smart card from the smart card reader while wiping it may result in unpredictable behavior.

3. Do one of the following:
   - Click the gold card icon found in the lower left corner of the PGPkeys window.
   - Select **Smart Card Properties** from the **View** menu.

   The Smart Card window appears.
4. Click the **Contents** tab.

   The Contents tab appears, showing the keys stored on your smart card.
5. Click the **Wipe Contents** button.

   PGP asks for a confirmation that you want to delete all keys currently on the card.

Caution: Once you wipe the smart card, you will not be able to retrieve any keys that were previously stored on the card. This includes any keypairs, or private keys you created on the card. If you delete the private portion of your keypair, then you will not be able to decrypt any data encrypted to it.

6. To wipe the contents of the smart card, click **OK**.

   The PGP Enter Passphrase screen appears.
7. Enter the PIN for this smart card.

   Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the **Hide Typing** check box.
8. Click **OK**.

   PGP deletes all keys stored on the smart card.

Copying a keypair from your keyring to a smart card

PGP also lets you copy an existing keypair from your desktop to a smart card. This is a good way to make a usable backup of your keypair; you can also use the copy on your smart card to copy your public key to other people's keyring (see "Copying your public key from a smart card to someone's keyring" on page 69 for more information).

Note that copying your keypair to a smart card is different from creating a keypair directly on the smart card. When you create a keypair directly on a smart card, you must have the smart card on the system to use your private key.

When you have a keypair on your desktop and copy it to a smart card, things work slightly differently. In this case, the private portion of your keypair resides on the smart card **and on your desktop** (unless you choose to delete the private portion of your keypair from your system).

There are two main reasons to copy an existing keypair to your smart card:

- to use it as a backup for the keypair on your system and to copy your public key from the smart card to other people's keyrings. In this case, you would have two copies of the same private key: one on the system where you originally created it and one on the smart card.
- to use it as your only copy of your private key, just as if you'd created it directly onto the smart card. In this case, you would need to delete the private key from your system (PGP gives you the option to do this). You would select this option if you started using smart cards after you had already created your PGP keypair and wanted to have the advantages of having your keypair on your smart card but didn't want to create a new keypair.

Finally, when you copy your PGP keypair to a smart card, the passphrase for the keypair that's on the smart card is automatically changed from whatever it was to the PIN of the smart card. However, the passphrase for the keypair that was already on your system, the keypair you copied to the smart card, doesn't change. Thus you end up with two copies of the same exact keypair, each with their own passphrase.

If you decide to delete the private key from your system and just keep the private key on your smart card, this isn't a problem; you just use the PIN of the smart card as the passphrase for your private key.

If, however, you choose to keep both keypairs, then use the passphrase for the keypair on your system; it takes precedence over the passphrase of the smart card.

To copy an existing PGP keypair to your smart card:

1. Put your smart card in the smart card reader.

Caution: Removing your smart card from the smart card reader while copying keys to the smart card may result in unpredictable behavior.

2. Open PGPkeys.
3. Select the keypair you want to copy to your smart card.

   Diffie-Hellman/DSS keys are not supported on smart cards.
4. Pull down the Server menu and choose **Send To –> Smart Card**.

   A note appears informing you that once the keypair is copied to the smart card, your PGP passphrase for this keypair will automatically change to the PIN belonging to the smart card.
5. Click **OK** to continue.

   The PGP Enter Passphrase screen appears.
6. Enter the passphrase for your key, then click **OK**.

   The PGP Enter Passphrase screen appears.
7. Enter the PIN for your smart card, then click **OK**.

   The keypair is copied to your smart card.

   PGP asks if you want to remove the private portion of the keypair from your keyring so that it only resides on the smart card.
8. Click **Yes** to remove the private portion of your keypair from your keyring; click **No** to leave the private portion of your keypair on your keyring.

   If you clicked Yes, the private portion of your keypair is deleted from the keyring on your system and exists only on your smart card.

   If you clicked No, the private portion is not deleted; you now have two copies of the same keypair, one on your system and the other on your smart card.

11 PGP Disk Basics

This chapter describes the basics of PGP Disk.

What is PGP Disk?

PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data. This reserved space is used to create a file called a PGPdisk *volume*.

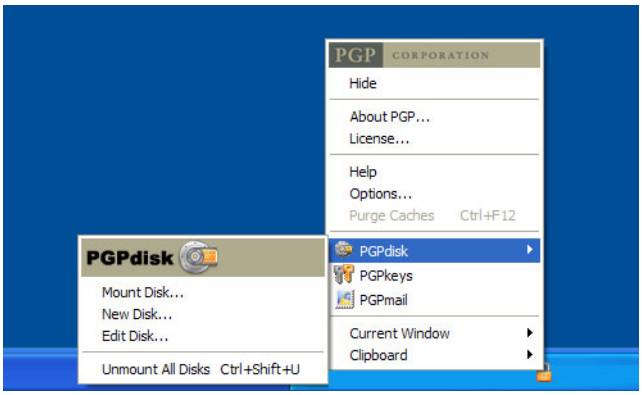
Although it is a single file, a PGPdisk volume acts very much like a hard disk in that it provides storage space for your files and applications. You can think of it like a floppy disk or an external hard disk. To use the applications and files stored in the volume, you *mount* it or make it accessible to you.

When a PGPdisk volume is *mounted*, you can use it as you would use any other disk. You can install applications within the volume or move or save your files to the volume. When the volume is *unmounted* it is inaccessible to anyone who does not know your secret passphrase. Even a mounted volume is protected; it is stored in encrypted format unless a file or application is in use. If your computer should crash while a volume is mounted, the volume's contents remain encrypted.

Accessing PGPdisk

PGPdisk can be accessed from PGPtray: click the **PGPtray** icon, slide up to **PGPdisk**, then slide over and select the appropriate command.

The PGPdisk menu from PGPtray provides a convenient means of creating and mounting volumes. A brief description of each option is listed below.



PGP Disk options are:

- **Mount Disk:** Mounts the specified PGPdisk volume provided that the correct passphrase is entered.
- **New Disk:** Displays the PGPdisk wizard, which guides you through the process of creating a new PGPdisk volume.
- **Edit Disk:** Opens the PGPdisk Editor, where you can perform administrative tasks to a PGPdisk volume.
- **Unmount All Disks:** Unmounts all existing PGPdisk volumes and stores them in encrypted format.

Working with PGPdisk in Windows Explorer

Windows Explorer can be used to perform the primary PGPdisk operations:

- Mounting PGPdisk volumes
- Unmounting already mounted PGPdisk volumes
- Creating, copying, moving, and deleting files and folders stored on your PGPdisk volume
- Accessing the PGPdisk Editor for a PGPdisk volume.

When a volume is unmounted, its contents remain secured in an encrypted file where it is inaccessible until the volume is once again mounted. The PGD file containing the PGPdisk contents can be stored on any disk drive in your system.

When a PGPdisk volume is mounted, it appears as an empty disk drive in a Windows Explorer window so you can start working in it immediately.

To mount a PGPdisk volume in Windows Explorer:

1. Locate and select the encrypted volume file you want to mount from the Windows Explorer folder tree.
2. Right-click on the encrypted volume's file name to display the Context menu.
3. Select **PGP—>Mount PGPdisk**.
4. Enter the passphrase, and click **OK**.

To unmount a PGPdisk volume in Windows Explorer:

1. Locate and select the PGPdisk volume you want to unmount in the Windows Explorer folder tree.
2. Right-click on the mounted volume's file name to display the Context menu.
3. Select **PGP—>Unmount PGPdisk**

Creating a new PGPdisk volume

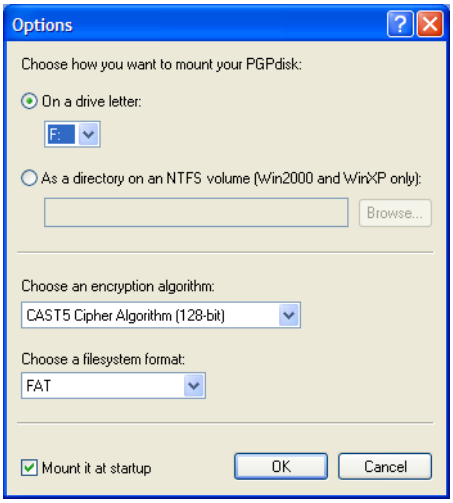
To create a new PGPdisk volume:

1. Select **Start —>Programs—>PGP—>PGPdisk.**
2. The **PGPdisk Wizard** appears on your screen. Read the introductory information.
3. Click **Next**. A dialog box appears that allows you to identify the location and size of the new volume.
4. Click **Browse** to navigate to a destination directory for your PGPdisk volume or accept the default location.
   - Windows 95: The default location is C:\My Documents\
   - Windows NT: The default location is C:\WINNT\Profiles\{Name of Current User}\Personal\
   - Windows 98: The default location is C:\My Documents\
   - Windows ME: The default location is C:\My Documents\
   - Windows 2000: The default location is C:\Documents and Settings\{Name of Current User}\My Documents\
   - Windows XP: The default location is C:\Documents and Settings\{Name of Current User}\My Documents\
5. Enter the amount of space you want to reserve for the new volume (**PGPdisk Size field**). Use whole numbers, no decimal places. You can use the arrows to increase or decrease the number displayed in the field.

   The amount of free disk space for the selected drive is shown above the **Size** field.
6. Choose **KB** (kilobytes), **MB** (megabytes), or **GB** (gigabytes) from the size list.

   You can create a volume of any size larger than 100 kilobytes. The maximum allowable size for a PGPdisk volume depends on your version of Windows and on the size and format of your hard disk.
7. Click **Advanced Options** to specify where and how you want to mount your PGPdisk.

   The **Options** dialog box appears.



8. Select the desired options from the appropriate check boxes and lists:

   – **On a drive letter.** Select the drive letter where you want to mount your new PGPdisk volume. A list of available drives appears in the drive letter list. Your new PGPdisk volume appears at this location in your Windows Explorer folder tree when mounted.

   – **As a directory on an NTFS volume.** This option is only available on Windows 2000 systems. Click this option if you want to mount your new PGPdisk volume as a directory on an NTFS volume. Type the path to an empty directory in the space provided or browse to the desired location.

     If you enter a path to a non-existing directory on an NTFS volume, you will be asked if you want to create a directory by that name. Select **Yes**, then enter your passphrase. The directory appears in Windows Explorer on the NTFS volume you selected.

Note: Right-click on a drive letter in Windows Explorer, and select **Properties** to identify the file format for that drive.

   – **Choose an encryption algorithm.** Select the encryption algorithm you want to use to protect your data.

     CAST5 Cipher Algorithm (128-bit). CAST is a 128-bit block cipher. It is a strong, military-grade encryption algorithm that has a solid reputation for its ability to withstand unauthorized access.

     Twofish Cipher Algorithm (256-bit). Twofish is a new 256-bit block cipher, symmetric algorithm. It was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).

- **Choose a filesystem format.** Specify a file system format for the new PGPdisk volume.

  FAT. (available on all Windows platforms)

  NTFS. (Windows NT, 2000, and XP platforms, only available for PGPdisk volumes larger than 5MB)

  FAT32. (Windows 95, Windows 98 and Windows 2000 platforms, only available for PGPdisk volumes larger than 260 MB)

- **Mount at startup.** Check this option to mount PGPdisk volumes at startup. When checked, you are prompted for your PGPdisk passphrase at startup.

9. Click **OK.** This closes the **Advanced Options** dialog box.
10. Click **Next**.
11. Choose a protection method for your new PGPdisk volume. Select one of the following options.

    - **Public key.** If you choose to protect your PGPdisk with a public key, a list of the public keys on your keyring will appear. Select the key you want to use to protect your new PGPdisk volume.
    - **Passphrase.** If you choose to protect your PGPdisk with a passphrase, you must also enter a user name.

      Enter the string of words or characters that serves as your passphrase to access the new volume (also called the volume's master passphrase). To confirm your entry, press Tab to advance to the next text box, then enter the same passphrase again. The suggested minimum size for a passphrase is eight characters.

      Normally, as an added level of security, the characters you enter for the passphrase are not visible on the screen. However, if you are sure that no one is watching (either physically or over the network) and you would like to see the characters of your passphrase as you type, click the **Hide Typing** box.

Note: Your security is only as good as your passphrase.

12. Click **Next**. A progress bar indicates how much of the PGPdisk volume has been initialized and formatted.
13. Click **Next** to mount your PGPdisk.
14. Click **Finish** to begin working with your new PGPdisk volume.

    Your PGPdisk volume appears in a Windows Explorer window.

Mounting a PGPdisk volume

When you create a new volume, the PGPdisk program automatically mounts it so you can begin using it to store your files. When you are ready to secure the contents of the volume, you must unmount it. Once a volume is unmounted, its contents remain secured in an encrypted file where it is inaccessible until the volume is once again mounted.

There are several ways to mount a PGPdisk volume:

- Find the file for the PGPdisk in Windows Explorer and double click it.
- In Windows Explorer, right-click the PGPdisk file, and select **PGP—>Mount PGPdisk.**
- In PGPtray, select **PGPdisk—>Mount Disk**.
- In the PGPdisk Editor, click the **Mount** button or select **Mount** from the **File** menu.

The mounted PGPdisk volume appears on an empty drive in a Windows Explorer window.

Using a mounted PGPdisk volume

You can create, copy, move, and delete files and folders on a PGPdisk volume just as you normally do with any other volume. Similarly, anyone else who has access to the volume (either on the same machine or perhaps over the network) can also access the data stored in the volume. It is not until you unmount the volume that the data in the encrypted file associated with the volume is made inaccessible.

Caution: Although the encrypted file associated with each volume is safe from snooping, it can still be deleted. If an unauthorized person is able to access your data, he or she could potentially delete the encrypted file upon which the volume is based. It is a good idea to keep a backup copy of the encrypted file.

Unmounting a PGPdisk volume

After you are through accessing a given volume and you want to lock its contents, you need to unmount the volume.

Caution: You may lose data if you unmount a PGPdisk volume that contains open files. If you select **Allow forcible unmounting of PGPdisks with open files** and **Don't ask before forcibly unmounting a PGPdisk** from the **PGP Options** panel, then you will not receive a warning before unmounting a volume that contains open files and you risk losing the data stored in the volume. For more information on setting PGP options, see "Setting PGPdisk options" on page 73.

There are several ways to unmount a volume:

- In Windows Explorer, right-click on the PGPdisk file, and select **PGP—> Unmount PGPdisk**.
- In the PGPdisk Editor, click the **Unmount** button or select **Unmount** from the **File** menu.
- In PGPtray, select **PGPdisk—>Unmount All Disks**.
- Enable a key shortcut (the default is Ctrl-Shift-U) to unmount all PGPdisks. For details more information, see "Setting HotKey options" on page 65.

Once a volume is unmounted, its contents are locked in the encrypted file associated with the volume. The contents of the volume are stored in the encrypted file and its contents remain inaccessible until the volume is once again mounted. It may help to view PGPdisk volumes as a window that provides a view to the data in the encrypted file. The contents of a PGPdisk volume file only become available when the file is mounted as a volume by someone who knows a valid passphrase.

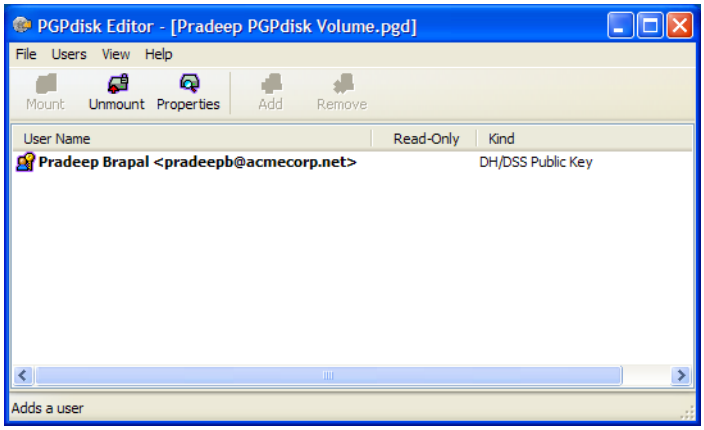
12 Using PGP Disk

This chapter explains how to create, mount and unmount existing PGPdisk volumes and how to specify properties that protect volume contents by unmounting them under certain circumstances.

Working with PGPdisk in a PGPdisk Editor

The PGPdisk Editor is used for administrative tasks you perform on your PGPdisk volume. For example:

- Changing a passphrase
- Adding and removing alternate users
- Setting read-only status
- Mounting PGPdisk volumes
- Unmounting already mounted PGPdisk volumes
- Specifying PGP Options
- Specifying PGP Properties for mounting the PGPdisk volume at startup or for re-encrypting your volume.



The PGPdisk Editor displays the list of users who are allowed to access the volume and their method of authentication: public key or passphrase. An icon appears next to the name of the administrator for the volume. The PGPdisk Editor can be accessed from Windows Explorer or from PGPtray.

To access the PGPdisk Editor from Windows Explorer:

1. Locate and select the encrypted volume file you want to modify in the Windows Explorer folder tree.
2. Right-click on the encrypted volume's file name to display the Context menu.
3. Select **PGP—>Edit PGPdisk**.

To access the PGPdisk Editor from PGPtray:

1. In PGPtray, select **PGPdisk—>Edit Disk**.
2. Locate and select the encrypted volume you want to modify, then click **Open**.

Changing a passphrase for a PGPdisk volume

Any user who knows a passphrase can change that passphrase, but the administrator always has access to the contents of the volume.

Note: If you choose to protect your PGPdisk volume with a PGP key, then you must go into PGPkeys to change the passphrase for your private key. You cannot change it from the PGPdisk Editor.

To change your passphrase:

1. Ensure that the PGPdisk volume is not mounted. You cannot change a passphrase if the PGPdisk volume is mounted.
2. Open the PGPdisk Editor for the volume you want to modify, then select the user name that applies to the passphrase you are changing.
3. Select **Change Passphrase** from the **Users** menu.

   The **Passphrase** dialog box appears.
4. Enter your passphrase, then click **OK**.

   The **Enter New Passphrase** window appears.
5. Enter the string of words or characters that serves as your new passphrase to access the new volume (also called the administrator's passphrase). To confirm your entry, press **Tab** to advance to the next text box, then enter the same passphrase again. The suggested minimum length for a passphrase is eight characters.
6. Click **OK**.

   The **New Passphrase** dialog box closes. The passphrase has been changed.

Adding alternate users to a PGPdisk volume

The PGPdisk administrator can make the PGPdisk available to other users. The users can access the volume using their own unique passphrase or private key. Only the person who knows the administrator passphrase can add alternate users.

You also have the option of assigning a read-only status to the volume. This allows alternate users to read the files but prevents them from altering the files in any way.

To add alternate users:

1. Ensure that the PGPdisk volume is not currently mounted. You cannot add alternate users while the PGPdisk volume is mounted.
2. Open the PGPdisk Editor for the volume you want to modify, then select **Add** from the **User** menu.

   The Passphrase dialog box appears, asking you to enter the administrator's passphrase.
3. Enter the administrator passphrase and click **OK**.

   The **PGPdisk User Creation Wizard** appears. Read the introductory information.
4. Click **Next**.
5. Choose a protection method for the new user. Select one of the following:
   - **Public key.** If you choose to protect the PGPdisk with a public key, a list of the public keys on your keyring appears. Highlight the alternate user's public key.

Note: Public key is the most secure protection method when adding alternate users to a PGPdisk volume because: (1) You don't need to exchange a passphrase with the alternate user which, depending on your method, could be intercepted or overheard. (2) The alternate user doesn't need to memorize another passphrase which could be forgotten. (3) It is easier to manage a list of alternate users if each uses his or her own private key to gain access to the volume.

   - **Passphrase.** If you choose to protect your PGPdisk with a passphrase, you must also enter the name of the alternate user.

     Enter the string of words or characters that serves as the passphrase to access the new volume. To confirm your entry, press Tab to advance to the next text box, then enter the same passphrase again. The suggested minimum size for a passphrase is eight characters.

Normally, as an added level of security, the characters you enter for the passphrase are not visible on the screen. However, if you are sure that no one is watching (either physically or over the network) and you would like to see the characters of your passphrase as you type, click the **Hide Typing** box.

Note: Your security is only as good as your passphrase.

6. Click **Next**. A progress bar indicates how much of the PGPdisk volume has been initialized and formatted.
7. Click **Finish**. The alternate user has been added.

   Once you have added an alternate user, you can remove the alternate user by choosing **Remove** from the **User** menu.

To assign read-only status:

1. Open the PGPdisk Editor for the volume you want to modify, then select the user name.
2. Select **Toggle Read-Only** from the **User** menu.

   The Passphrase dialog box appears, prompting you to enter the administrator's passphrase.
3. Enter the administrator passphrase, then click **OK**.

   A red dot appears next to the user's name in the **Read-Only** column.

   Once you have assigned read-only status to a user, you can remove the restriction by repeating the steps above.

Removing alternate users from a PGPdisk volume

Removing alternate users is similar to adding alternate users or changing a passphrase.

To remove alternate users:

1. Ensure that the PGPdisk volume is not mounted. You cannot remove alternate users if the PGPdisk volume is mounted.
2. Open the PGPdisk Editor for the volume you want to modify, then select the user name you want to remove from the list.
3. Select **Remove from the User menu**.

   The **Passphrase** dialog box appears, prompting you for either the administrator passphrase or the passphrase for the user being removed.
4. Enter the passphrase, and then click **OK**. The user has been removed.

Specifying properties for a PGPdisk volume

The **Properties** button in the PGPdisk Editor allows you to identify mounting options, as well as view which encryption algorithm is being used for that specific volume, and gives you the option to re-encrypt the volume. If you want to set PGP options which relate to all PGPdisk volumes, see "Setting PGP Disk options" on page 158.

To specify properties:

1. Open the PGPdisk Editor for the volume you want to modify, then click the **Properties** button or select **Properties** from the **File** menu.

   The **Properties** dialog box appears.

2. Select the desired options by clicking the appropriate check boxes.

   – **Re-Encrypt.** If selected, this option allows you to change the encryption algorithm of the PGPdisk, or re-encircle your PGPdisk with the same encryption algorithm to change your underlying encryption key. This may be necessary if you feel that the security of your PGPdisk has been compromised, or if you have removed a user from the PGPdisk and want to make absolutely sure he can never access it again.

Caution: An adept user may be able to search his computer's memory for the PGPdisk's underlying encryption key and save it in order to continue accessing the PGPdisk even if he was removed from the user list. Re-encryption changes this underlying key and prevents him from gaining access.

   – **Mount at startup**. Check this option to mount the PGPdisk volume at startup. When checked, you are prompted for your PGPdisk passphrase at startup.

   – **Override global auto-unmount setting**. When checked, this option allows you to override the global auto-unmount setting originally specified in the **PGP Options** panel for the selected PGPdisk volume.

Note: The global auto-unmount setting in the **PGP Options** panel applies to all mounted PGPdisk volumes. If you want a PGPdisk volume to auto-unmount at a different time than the time specified in the global auto-unmount setting, then you must choose to override it.

   The Auto unmount after [15] minutes of inactivity option is available when you have selected to override the global auto-unmount setting. This option allows PGP to automatically unmount the PGPdisk volume when your computer is inactive for the specified time. You can set this value from 1 to 999 minutes.

Maintaining PGPdisk volumes

This section describes how to automatically mount PGPdisk volumes when you start your system, how to back-up and exchange the data in these volumes with others, and how to re-encrypt your PGPdisk volume.

Automatically mounting PGPdisk volumes

You can automatically mount PGPdisk volumes when you first start your system.

There are two ways to automatically mount a volume:

- Check the **Mount at Startup** check box in the **Advanced Options** dialog box during the creation of your PGPdisk volume.
- Check the **Mount at Startup** check box in the **Properties** dialog box of the PGPdisk Editor for the volume you want to automatically mount.

Mounting PGPdisk files on a remote server

You can place PGPdisk volumes on any kind of server (Windows or UNIX) and allow them to be mounted by anyone with a Windows machine.

Note: The first person to mount the volume locally has read-write access to the volume. No one else is then able to access the volume. If you want others to be able to access files within the volume, you must mount the volume in read-only mode (applies to FAT and FAT32 filesystem formats only). *All* users of the volume then have read-only access.

If the volume is stored on a Windows server, you can also mount the volume remotely on the server and allow people to share the mounted volume. However, this action provides no security for the files within the volume.

Backing up PGPdisk volumes

You may want to back up the contents of your PGPdisk volumes to safeguard your information from system corruption or disk failures. While it is possible to back up the contents of a mounted PGPdisk volume just as you would any other volume, it is probably not a good idea because the contents are not encrypted and will thus be accessible to anyone who can restore the back up. Instead of backing up the contents of the mounted PGPdisk volume, you should make a back up of the encrypted PGPdisk volume.

To back up PGPdisk volumes:

1. Unmount the PGPdisk volume.

2. Copy the unmounted encrypted file to a floppy disk, tape, or removable cartridge just as you would any other file. Even if some unauthorized person has access to the backup, he or she will not be able to decipher its contents.

   When making backups of the encrypted files, keep these issues in mind:

   – PGPdisk is a product for security-minded people and organizations. Backing up the encrypted files to a network drive gives others plenty of opportunity to guess at a weak passphrase. We recommend that you back up only to devices over which you have physical control. A lengthy, complicated passphrase helps further reduce the risk in this situation.

   – If you are on a network, make sure that any network back up system does not back up your mounted volumes. You may need to discuss this with your System Administrator. Under some circumstances, you may not mind if backups are made of your encrypted files because this information is secure. Under no circumstances is it a good idea to allow the contents of your mounted volumes to be backed up, as this defeats the whole purpose of keeping this information encrypted.

Exchanging PGPdisk volumes

You can exchange PGPdisk volumes with colleagues who have their own PGPdisk program by sending them a copy of the encrypted file that contains the data associated with the volume. Here are some of the ways you might exchange PGPdisk volumes:

- As mail attachments
- On floppy disks or CD-Rs
- Over a network

Note: Public key is the most secure protection method when adding alternate users to a PGPdisk volume because: (1) You don't need to exchange a passphrase with the alternate user which, depending on your method, could be intercepted or overheard. (2) The alternate user doesn't need to memorize another passphrase which could be forgotten. (3) It is easier to manage a list of alternate users if each uses his or her own private key to gain access to the volume. The more security precautions you take, the greater assurance you have that your sensitive information remains confidential.

Once the intended party has a copy of the encrypted file, all they need in order to gain access to the contents of the volume is to mount it using the correct passphrase, or, if the volume was encrypted to their public key, their private key. They also need a copy of the PGPdisk program. For more information on how to mount a PGPdisk volume, see "Mounting a PGPdisk volume" on page 35.

Changing the size of a PGPdisk volume

While you cannot change the size of a PGPdisk volume once it has been created, you can create a larger or smaller volume and then copy the contents from the old volume to the new one.

To change the size of a PGPdisk volume:

1. Create a new PGPdisk volume and specify the desired size. For more information on how to create a new volume, see "Creating a new PGPdisk volume" on page 27.
2. Copy the contents of the existing mounted PGPdisk volume into the newly created volume.
3. Unmount the old PGPdisk volume and then delete the encrypted file associated with the volume to free up the disk space.

Re-encrypting a PGPdisk volume

PGP allows you to re-encrypt all data stored on a PGPdisk. This feature provides an additional level of protection in environments requiring a higher level of security. With re-encryption you can change the encryption algorithm used to protect the volume, or re-encrypt your PGPdisk with the same encryption algorithm to change your underlying encryption key.

Caution: An adept user may be able to search his or her computer's memory for the PGPdisk's underlying encryption key and save it in order to continue accessing the PGPdisk even if he or she was removed from the user list. Re-encryption changes this underlying key and prevents him from gaining access.

To re-encrypt a PGPdisk volume:

1. Open the PGPdisk Editor for the volume you want to modify, then click the **Properties** button or select **Properties** from the **File** menu.

   The **Properties** dialog box appears.
2. Click the **Re-Encrypt** button.
3. Enter your passphrase for the volume.

   The **PGPdisk Re-Encryption Wizard** appears.
4. Read the introductory information, and click **Next**.

   A dialog box appears displaying the current encryption algorithm protecting your PGPdisk volume and the new encryption algorithm.

   For example, if your PGPdisk is currently encrypted with CAST, then Twofish appears in the New Algorithm list, and vice-versa.

5. Choose from one of the following options:
   - Select the **Re-encrypt to the same algorithm** check box to re-encrypt the PGPdisk using the current algorithm, then click **Next**.
   - Click **Next** to re-encrypt the PGPdisk with the algorithm displayed in the **New Algorithm** drop-down list.

   The PGPdisk re-encrypts using the encryption algorithm you selected.
6. When the current status displays **Done**, click **Next**.
7. Click **Finish** to complete the re-encryption process.

13 PGP Disk Technical Details

This chapter discusses encryption and security issues and provides user tips and other technical information about PGPdisk.

About PGPdisk volumes

You can use PGPdisk volumes to organize your work, keep similarly named files separate, or keep multiple versions of the same documents or programs separate.

Although the volumes you create with PGPdisk function just as any other volume you are accustomed to working with, the data is actually stored in one large encrypted file. Only when you mount the file, are its contents are presented in the form of a volume. It is important to realize that all of your data remains secure in the encrypted file and is only deciphered when you access one of the files. Having the data for a volume stored in this manner makes it easy to manipulate and exchange PGPdisk volumes with others but it also makes it easier to lose data if the file is somehow deleted. It is wise to keep a back up copy of these encrypted files so that the data can be recovered in case something happens to the original.

It is also important to note that you cannot compress an encrypted file in an attempt to reduce its size, but you can compress the individual files contained in the mounted volume and thereby store more encrypted data in the volume. You can also store one secure PGPdisk volume within another and thus nest several volumes for an added level of security.

The PGPdisk encryption algorithms

Encryption employs a mathematical formula to scramble your data so that no one else can use it. When you apply the correct mathematical key, you unscramble the data. The PGPdisk encryption formula uses random data for part of the encryption process. Some of this random data comes from the movement of your mouse during encryption and some random data comes directly from your passphrase.

The PGPdisk program offers two strong algorithm options for protecting your PGPdisk volumes: CAST and Twofish.

CAST is considered an excellent block cipher because it is fast and very difficult to break. Its name is derived from the initials of its designers, Carlisle Adams and Stafford Tavares of Northern Telecom (Nortel). Nortel has applied for a patent for CAST, but they have made a commitment to make CAST available to anyone on a royalty-free basis. CAST appears to be exceptionally well-designed by people with good reputations in the field.

The design is based on a very formal approach, with a number of formally provable assertions that give good reasons to believe that it probably requires key exhaustion to break its 128-bit key. CAST has no weak keys. There are strong arguments that CAST is immune to both linear and differential cryptanalysis, the two most powerful forms of cryptanalysis in the published literature, both of which have been effective in cracking the Data Encryption Standard (DES).

Twofish is a relatively new, but well regarded 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the new Advanced Encryption Standard (AES).

Special security precautions taken by PGPdisk

PGPdisk takes special care to avoid security problems that other programs may not. These include the following:

Passphrase erasure

When you enter a passphrase, PGPdisk uses it only for a brief time, then erases it from memory. PGPdisk also avoids making copies of the passphrase. The result is that your passphrase typically remains in memory for only a fraction of a second. This feature is crucially important — if the passphrase remained in memory, someone could search for it in your computer memory while you were away from the machine. You would not know it, but they would then have full access to any PGPdisk volumes protected by this passphrase.

Virtual memory protection

Your passphrase or other keys could be written to disk as part of the virtual memory system swapping memory to disk. PGPdisk takes care that the passphrases and keys are never written to disk. This feature is important because someone could scan the virtual memory file looking for passphrases.

Memory Static Ion Migration Protection

When you mount a PGPdisk, your passphrase is turned into a key. This key is used to encrypt and decrypt the data on your PGPdisk volume. While the passphrase is erased from memory immediately, the key (from which your passphrase cannot be derived) remains in memory while the disk is mounted. This key is protected from virtual memory; however, if a certain section of memory stores the exact same data for extremely long periods of time without being turned off or reset, that memory tends to retain a static charge, which could be read by attackers. If your PGPdisk is mounted

for long periods, over time, detectable traces of your key could be retained in memory. Devices exist that could recover the key. You won't find such devices at your neighborhood electronics shop, but major governments are likely to have a few.

PGPdisk protects against this by keeping two copies of the key in RAM, one normal copy and one bit-inverted copy, and inverting both copies every few seconds.

Other security considerations

In general, the ability to protect your data depends on the precautions you take, and no encryption program can protect you from sloppy security practices. For instance, if you leave your computer on with sensitive files open when you leave your desk, anyone can access that information or even obtain the key used to access the data. Here are some tips for maintaining optimal security:

- Make sure that you unmount PGPdisk volumes when you leave your computer. This way, the contents will be safely stored in the encrypted file associated with the volume until you are ready to access it again.
- Use a screen saver with a password so that it is more difficult for someone to access your machine or view your screen when you are away from your desk.
- Make sure that your PGPdisk volumes cannot be seen by other computers on the network. You may need to talk to your network management people to guarantee this. The files in a mounted PGPdisk volume can be accessed by anyone who can see them on the network.
- Never write down your passphrases. Pick something you can remember. If you have trouble remembering your passphrase, use something to jog your memory, such as a poster, a song, a poem, a joke, but *do not write down your passphrases*.
- If you use PGPdisk at home and share your computer with other people, they will probably be able to see your PGPdisk files. As long as you unmount the PGPdisk volumes when you finish using them, no one else will be able to read their contents.
- If another user has physical access to your machine, that person can delete your PGPdisk files as well as any other files or volumes. If physical access is an issue, try either backing up your PGPdisk files or keeping them on an external device over which only you have physical control.
- Be aware that copies of your PGPdisk volume use the same underlying encryption key as the original. If you exchange a copy of your volume with another and both change your master passwords, both of you are still using the same key to encrypt the data. While it is not a trivial operation to recover the key, it is not impossible.

  You can change the underlying key by re-encrypting the PGPdisk volume.

14 Making Keys

This chapter describes how to generate the public and private keypairs that you need to correspond with other PGP users. It also explains how to distribute your public key and obtain the public keys of others.

Choosing a key type

PGP provides you with two key types to choose from: Diffie-Hellman/DSS and RSA. Versions of PGP prior to 5.0 used RSA keys exclusively. Versions later than 5.0 introduced the ElGamal variant of Diffie-Hellman technology.

With PGP versions 7.0 and above, the RSA key format has been improved to provide support for features previously available only to Diffie-Hellman/DSS keys: support for Additional Decryption Keys (ADKs), designated revokers, multiple encryption subkeys, and photo ID features. These features are not available to users with RSA keys created prior to Version 7.0, now known as RSA Legacy keys.

Which key type is the right choice for you?

- Choose **Diffie-Hellman/DSS** or **RSA** if you want to take advantage of many PGP key features: Additional Decryption Keys (ADKs), designated revokers, multiple encryption subkeys, and photo IDs.
- Choose **RSA** or **RSA Legacy** if you plan to correspond with people who are using RSA keys.
- Choose **RSA Legacy** only if those you communicate with are using older versions of PGP; otherwise, choose the new RSA key format. (The two formats are not compatible with each other.)

Note: The RSA key type is only fully compatible with PGP versions 7.0 and above, and other OpenPGP applications.

If you plan to correspond with people who are still using RSA Legacy keys, you might want to generate an RSA Legacy keypair, which is compatible with older versions of the program. If you need to, you can generate more than one keypair.

Making a keypair

Unless you have already done so while using another version of PGP, the first thing you need to do before sending or receiving encrypted and signed email is create a new keypair. You generate a new keypair from PGPkeys using the PGP Key Generation Wizard, which guides you through the process.

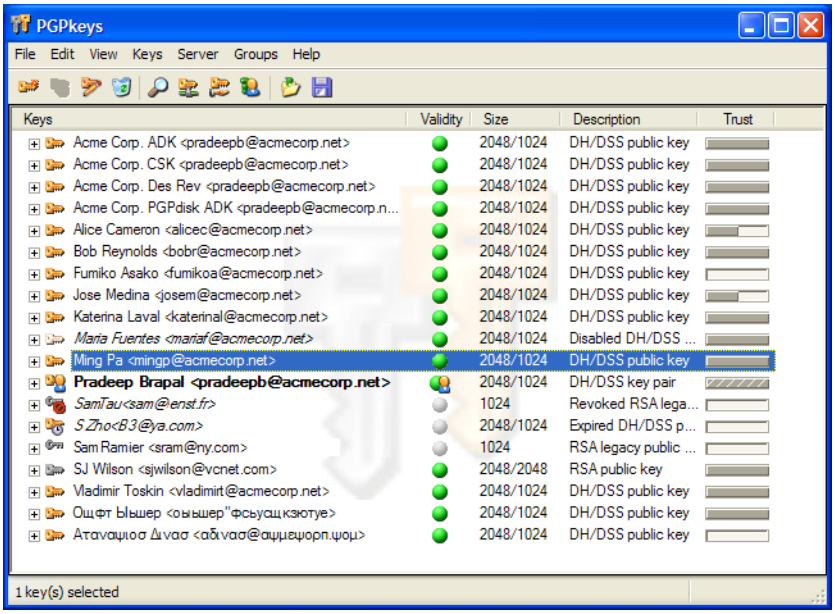
If you have an existing keypair, specify the location of your keys when you run the PGPkeys application. You can go to the Files tab of the Options screen and locate your keyring files at any time.

Caution: Although it's fun, do not create more than one keypair unless you need to. When another user wants to send you email, it might confuse them if you have more than one keypair. Also, you might not remember all of the passwords for each keypair.

To create a new keypair:

1. Open PGPkeys. You can open PGPkeys by:
   - Double-clicking the PGPkeys icon in the PGP folder.
   - Clicking **Start—>Programs—>PGP—>PGPkeys**
   - Clicking the PGPtray icon ( ) in the System tray, then selecting **PGPkeys**.
   - Clicking in your email application's toolbar

The PGPkeys window displays the private and public keypairs you have created for yourself, as well as any public keys of other users that you have added to your public keyring. It is from this window that you will perform all future key management functions.



Note: Depending on your situation, the PGPkeys window may be empty, or it may be pre-configured by your PGP administrator to display specific keys.

2. Click in the PGPkeys menu bar.

   The PGP Key Generation Wizard provides some introductory information on the first screen.

3. After you read the introductory information, click **Next** to advance to the next panel.

   The PGP Key Generation Wizard asks you to enter your name and email address.

4. Enter your name in the Full Name box and your email address in the Email Address box, then click **Next**.

   It is not absolutely necessary to enter your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and others can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient.

5. If PGP detects that your computer is in a Microsoft Exchange Server environment or if your PGP administrator has configured PGP to include specific installation settings, the Administrator Options panel appears. Read the information on this panel, then click **Next** to continue.
6. On the Passphrase screen, enter the string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press the Tab key to advance to the next field, then enter the same passphrase again. For more information on creating an effective passphrase, see "Creating a passphrase you will remember" on page 103.

   Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the Hide Typing check box.

Caution: Unless your PGP administrator has implemented a PGP key reconstruction policy for your company, no one, including PGP Corporation, can salvage a key with a forgotten passphrase.

7. Click **Next** to begin the key generation process.

   If you have entered an inadequate passphrase, a warning message appears before the keys are generated. Depending on the PGP settings specified by your administrator, you may have the choice of accepting the bad passphrase or entering a more secure one before continuing.

   Your mouse movements and keystrokes generate random information that is needed to create a unique keypair. If there is not enough random information upon which to build the key, the PGP Random Data screen appears. As instructed in the dialog box, move your mouse around and enter a series of random keystrokes until the progress bar is completely filled in.

Note: PGP continually gathers random data from many sources on the system, including mouse positions, timings, and keystrokes. If the Random Data screen does not appear, it indicates that PGP has already collected all the random data that it needs to create the keypair.

   If you are in a Microsoft Exchange Server environment, PGP informs you that it needs to retrieve your email user ID from your Exchange server in order to add it to your new PGP key. If this is the case, continue with the instructions outlined in "Adding your email ID from your Microsoft Exchange Server to your new key" on page 102.
8. When the key generation process indicates that it is done, click **Next**.
9. Click **Finish**. PGP automatically puts your private key on your private keyring and your public key on your public keyring.

Once you have created a keypair, you can use PGPkeys to create new keypairs and manage all of your other keys. For instance, this is where you examine the attributes associated with a particular key, specify how confident you are that the key actually belongs to the alleged owner, and indicate how well you trust the owner of the key to vouch for the authenticity of other users' keys. For a complete explanation of the key management functions you perform from the PGPkeys window, see Chapter 16, Managing Keys.

Generating a custom key

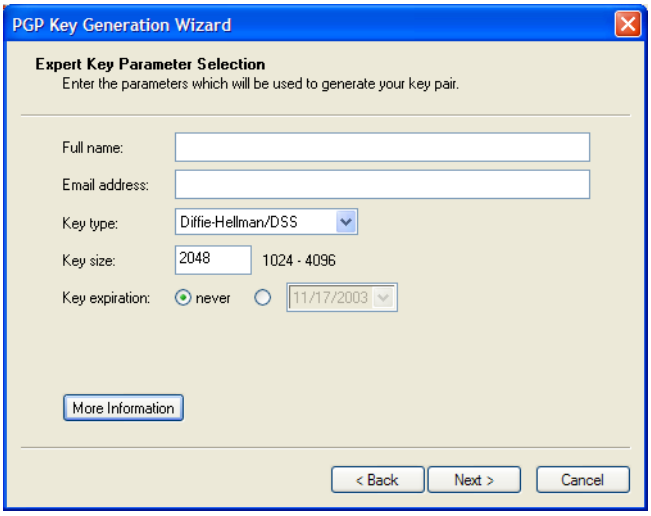
If you want to specify the type of key to generate, specify a key size, and set an expiration date, then follow the instructions below on how to generate a custom key.

To generate a custom keypair:

To create a new keypair:

1. Open PGPkeys.
2. Click in the PGPkeys menu bar.
3. At the Key Generation Wizard Welcome screen, click the **Expert** button.

   The Key Generation Wizard Expert panel appears.



4. Enter your name in the Full Name box and your email address in the Email Address box.

   It is not absolutely necessary to enter your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, by using your correct email address, you and oth-

ers can take advantage of the plug-in feature that automatically looks up the appropriate key on your current keyring when you address mail to a particular recipient.

5. In the Key Type box, select the type of key you want to create. If you do not know which key type is the right choice for you, see "Choosing a key type" on page 95.
6. In the Key Size box, select the number of bits you want your new key to be made of. For Diffie-Hellman/DSS or RSA keys, select a key size from 1024 to 4096 bits. For RSA Legacy keys, select a key size from 1024 to 2048 bits.

Note: A large key size may take a long time to generate, depending on the speed of the computer you are using. It may also take a long time if you have Faster key generation turned off in the General tab of the PGP Options screen.

The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance that someone will be able to crack it, but the longer it takes to perform the decryption and encryption process. You need to strike a balance between the convenience of performing PGP functions quickly with a smaller key and the increased level of security provided by a larger key. Unless you are exchanging extremely sensitive information that is of enough interest that someone would be willing to mount an expensive and time-consuming cryptographic attack in order to read it, you are safe using a key composed of 1024 bits.

7. Indicate when you want your keys to expire. You can either use the default selection, which is Never, or you can enter a specific date after which the keys will expire.

   Once you create a keypair and have distributed your public key to the world, you will probably continue to use the same keys from that point on. However, under certain conditions you may want to create a special keypair that you plan to use for only a limited period of time. In this case, when the public key expires, it can no longer be used by someone to encrypt mail to you but it can still be used to verify your digital signature. Similarly, when your private key expires, it can still be used to decrypt mail that was sent to you before your public key expired but can no longer be used to sign mail to others.
8. Click **Next**.
9. If PGP detects that your computer is in a Microsoft Exchange Server environment or if your PGP administrator has configured PGP to include specific installation settings, the Administrator Options panel appears. Read the information in this panel, then click **Next** to continue.

10. In the Passphrase panel, enter the string of characters or words you want to use to maintain exclusive access to your private key. To confirm your entry, press the Tab key to advance to the next field, then enter the same passphrase again. For more information on creating an effective passphrase, see "Creating a passphrase you will remember" on page 103.

    Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, clear the **Hide Typing** check box.

Caution: Unless your administrator has implemented a PGP key reconstruction policy for your company, no one, including PGP Corporation, can salvage a key with a forgotten passphrase.

11. Click **Next** to begin the key generation process.

    The PGP Key Generation Wizard indicates that it is busy generating your key.

    If you have entered an inadequate passphrase, a warning message appears before the keys are generated and you have the choice of accepting the bad passphrase or entering a more secure one before continuing.

    Your mouse movements and keystrokes generate random information that is needed to create a unique keypair. If there is not enough random information upon which to build the key, the PGP Random Data screen appears. Move your mouse around and enter a series of random keystrokes until the progress bar is completely filled in.

Note: PGPkeys continually gathers random data from many sources on the system, including mouse positions, timings, and keystrokes. If the Random Data screen does not appear, it indicates that PGP has already collected all the random data that it needs to create the keypair.

    If you are in a Microsoft Exchange Server environment, PGP informs you that it needs to retrieve your email user ID from your Exchange server in order to add it to your new PGP key. If this is the case, continue with the instructions outlined in "Adding your email ID from your Microsoft Exchange Server to your new key" on page 102.

12. When the key generation process indicates that it is done, click **Next**.
13. Click **Finish**.

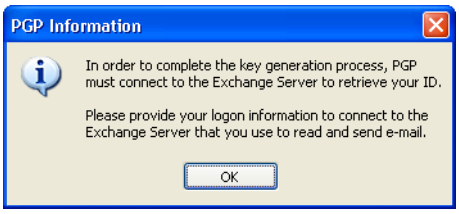
    PGP automatically puts your private key on your private keyring and your public key on your public keyring.

Adding your email ID from your Microsoft Exchange Server to your new key

If PGP detects that your computer is in a Microsoft Exchange Server environment, then PGP retrieves your email user ID from your Exchange server and adds it to your new PGP key during the key generation process.

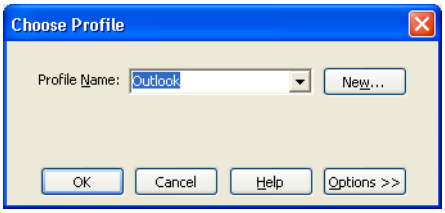
To retrieve your email ID from your Exchange Server:

1. During key generation, a PGP Information screen informing you that PGP must retrieve your user ID from your Exchange server appears.
2. Read the information, and click **OK**.


PGP Information
In order to complete the key generation process, PGP must connect to the Exchange Server to retrieve your ID.
Please provide your logon information to connect to the Exchange Server that you use to read and send e-mail.
OK

   The Choose Profile screen appears.

3. Select the user profile you want to connect to from the Profile Name box. This will likely be your company name.



4. Click **OK**.

   The Microsoft Exchange Server screen appears.

   The appearance of this screen varies depending on what version of Outlook you are using.

5. Enter the full name of your Exchange Server in the Microsoft Exchange server field and enter your user login name in the Mailbox field.
6. Click **Check Name**.

   If the login information is entered correctly, the names are underlined. If you do not know what Exchange Server you are on, or if the names did not underline, then contact your Microsoft Exchange administrator.

7. Click **OK**.

PGP continues the key generation process and adds your Microsoft Exchange email user ID to your new PGP key.

8. When the key generation wizard indicates that it is done, click **Next**.
9. Click **Finish**.

   PGP automatically puts your private key on your private keyring and your public key on your public keyring.

Creating a passphrase you will remember

Encrypting a file and then finding yourself unable to decrypt it is a painful lesson in learning how to choose a passphrase you will remember.

Most applications require a single word password between three and eight letters. For a couple of reasons we do not recommend that you use a single-word passphrase. A single word password is vulnerable to a dictionary attack, which consists of having a computer try all the words in the dictionary until it finds your password.

To protect against this manner of attack, it is widely recommended that you create a word that includes a combination of upper and lowercase alphabetic letters, numbers, punctuation marks, and spaces. This results in a stronger password, but an obscure one that you are unlikely to remember easily.

Trying to thwart a dictionary attack by arbitrarily inserting a lot of funny non-alphabetic characters into your passphrase has the effect of making your passphrase too easy to forget and could lead to a disastrous loss of information because you can't decrypt your own files. A multiple word passphrase is less vulnerable to a dictionary attack. However, unless the passphrase you choose is something that is easily committed to long-term memory, you are unlikely to remember it verbatim.

Picking a phrase on the spur of the moment is likely to result in forgetting it entirely. Choose something that is already residing in your long-term memory. It should not be something that you have repeated to others recently, nor a famous quotation, because you want it to be hard for a sophisticated attacker to guess. If it's already deeply embedded in your long-term memory, you probably won't forget it.

Of course, if you are reckless enough to write your passphrase down and tape it to your monitor or to the inside of your desk drawer, it won't matter what you choose.

Changing your keypair

Once you create your key, you can add, remove, or change a number of items in your keypair at any time.

Your private and public keys are stored in separate keyring files. You can copy them to another location on your hard drive or to a floppy disk. By default, the private keyring (secring.skr) and the public keyring (pubring.pkr) are stored along with the other program files in your "PGP" folder; you can save your backups in any location you like.

Note: Keys generated on a smart card cannot be backed up because the private portion of your keypair is non-exportable.

You can configure PGP to back up your keyrings automatically after you close PGP. Your keyring backup options can be set in the Advanced tab of the Options screen.

Protecting your keys

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your email or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the Internet.

To prevent anyone who might happen to intercept your passphrase from using your private key, store your private key only on your own computer. If your computer is attached to a network, make sure that your files are not automatically included in a system-wide backup where others might gain access to your private key. Given the ease with which computers are accessible over networks, if you are working with extremely sensitive information, you may want to keep your private key on a floppy disk, which you can insert like an old-fashioned key whenever you want to read or sign private information.

As another security precaution, consider assigning a different name to your private keyring file and then storing it somewhere other than in the default location. Use the Files tab of the Options screen to specify a name and location for your private and public keyring files.

PGP key reconstruction

If you lose your key or forget your passphrase and do not have a backed up copy from which to restore your key, you will never again be able to decrypt any information encrypted to your key. You can, however, reconstruct your key if your administrator has implemented a PGP key reconstruction policy for your company, where your key is encrypted and stored on a PGP key reconstruction server in such a way that only you can retrieve it.

A PGP key reconstruction server can be set up by your administrator to act as sort of a safety-net for you if you lose your private key or passphrase. The reconstruction server stores your key in such a way that only you can access it. Your company does not have the ability to decrypt your key.

If your administrator has incorporated key reconstruction as part of your company's security policy, you will be prompted to enter additional "secret" information when you create your PGP keypair or when you choose **Send to... Key Reconstruction Server** from the Server menu in PGPkeys. Your administrator may also supply you with a user ID and password so that you can log on to the key reconstruction server.

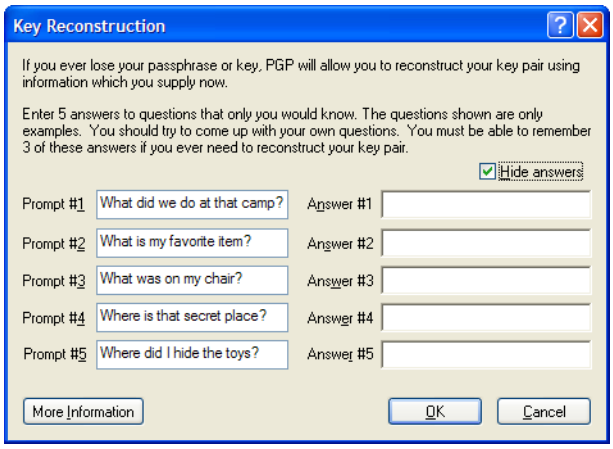
Once your key is on the server, you can restore it at anytime by selecting Reconstruct Key from the Keys menu in PGPkeys.

Note: You cannot reconstruct a key that was generated on a smart card because the private portion of the keypair is non-exportable.

To send your key to your company's key reconstruction server:

1. If the Key Reconstruction screen opened automatically as you created a keypair, continue with Step 3; otherwise, open PGPkeys and select your keypair.
2. Open the Server/Send To menu and select Reconstruction Server.

   The Key Reconstruction screen appears.


Key Reconstruction
If you ever lose your passphrase or key, PGP will allow you to reconstruct your key pair using information which you supply now.
Enter 5 answers to questions that only you would know. The questions shown are only examples. You should try to come up with your own questions. You must be able to remember 3 of these answers if you ever need to reconstruct your key pair.
Hide answers
Prompt #1
What did we do at that camp?
Answer #1
Prompt #2
What is my favorite item?
Answer #2
Prompt #3
What was on my chair?
Answer #3
Prompt #4
Where is that secret place?
Answer #4
Prompt #5
Where did I hide the toys?
Answer #5
More Information
OK
Cancel

3. On the Key Reconstruction screen, enter five questions that only you can answer in the Prompt boxes (the default questions are examples only). Choose obscure personal questions with answers that you are not likely to forget. Your questions can be up to 95 characters in length.

   An example of a good question might be, "Who took me to the beach?" or "Why did Fred leave?"

An example of a bad question would be, "What is my mother's maiden name?" or "Where did I go to high school?"

Note: If you prefer, you can also leave the questions blank and simply provide five answers.

4. In the Answer boxes, enter the answers to the corresponding questions. Your answers are case sensitive and can be up to 255 characters in length.

   Use the Hide Answers check box to view or hide your answers.

5. Click **OK** to continue.

   If the PGP Enter Passphrase for Key screen appears, enter the passphrase for your key, then click **OK**.

   If the Server User ID and Password screen appears, enter your user ID and password to log on to the server. If you do not know your user ID or password, consult your administrator.

6. Click **OK**.

   Your private key is split into five pieces, using Blakely-Shamir key splitting. Three of the five pieces are needed to reconstruct the key. Each piece is then encrypted with the *hash*, the uniquely identifying number, of one answer. If you know any three answers, you can successfully reconstruct the whole key.

15 Exchanging Keys

This chapter tells you about how to exchange keys; that is, how to distribute your public key (so that others can send you encrypted messages) and how to get the public keys of others (so that you can send encrypted messages to them). It also describes how to validate someone's public key.

The sections in this chapter are:

- Overview
- Distributing your public key
- Obtaining the public keys of others
- Validating keys

Overview

After you create your keypair, you need to exchange keys with those whom you intend to exchange encrypted messages. You make your public key available to others so that they can send you encrypted information and verify your digital signature; to send encrypted messages to them, you will need their public keys.

Your public key is basically composed of a block of text, so it is quite easy to make it available through a public keyserver, include it in an email message, or export or copy it to a file. The recipient can then use whatever method is most convenient to add your public key to his or her public keyring.

Finally, once you have someone's public key, you should validate it to make sure it belongs to the person to whom it's supposed to belong.

Distributing your public key

You can distribute your public key in various ways:

- Make your public key available through a public keyserver
- Include your public key in an email message
- Export your public key or copy it to a text file
- Copy your public key from a smart card directly to someone's keyring

Placing your public key on a keyserver

The best method for making your public key available is to place it on a public keyserver, which is a large database of keys, where anyone can access it. That way, people can send you encrypted email without having to explicitly request a copy of your key. It also relieves you and others from having to maintain a large number of public keys that you rarely use.

There are a number of keyservers worldwide, including those offered by PGP Corporation, where you can make your key available for anyone to access. If you are using PGP in a corporate setting, your PGP administrator will usually preconfigure your keyserver settings so that everything works correctly for your site.

When you're working with a public keyserver, such as keyserver.pgp.com, keep these things in mind before you send your key:

- Is this the key you intend to use? Others attempting to communicate with you might encrypt important information to that key. For this reason, we strongly recommend that you only put keys on a key server that you intend for others to use.
- Will you remember your passphrase for this key so you can retrieve data encrypted to it or, if you don't want to use the key, so you can revoke it?
- Once it's up there, it's up there. Some public servers have a policy against deleting keys. Others have replication features that replicate keys between keyservers, so even if you are able to delete your key on one server, it could reappear later.

To send your public key to a keyserver:

1. Open PGPkeys.
2. Select the public key to copy to the keyserver.
3. Open the Server menu, then select the keyserver on which you want to add your key from the Send To submenu. (The keyserver at PGP Corporation is ldap://keyserver.pgp.com.)

   PGP lets you know that the keys are successfully copied to the server.

Once you place a copy of your public key on a key server, it's available to people who want to send you encrypted data or to verify your digital signature. Even if you don't explicitly point people to your public key, they can get a copy by searching the key server for your name or email address.

Many people include the Web address for their public key at the end of their email messages. In most cases, the recipient can just double-click the address to access a copy of your key on the server. Some people even put their PGP fingerprint on their business cards for easier verification.

Including your public key in an email message

Another convenient method of delivering your public key to someone is to include it with an email message. When you send someone your public key, be sure to sign the email. That way, the recipient can verify your signature and be sure that no one has tampered with the information along the way. Of course, if your key has not yet been signed by any trusted introducers, recipients of your signature can only truly be sure the signature is from you by verifying the fingerprint on your key.

To include your public key in an email message:

1. Open PGPkeys.
2. Right click on your keypair, slide down to **Send To** on the context menu, then slide over and select **Mail Recipient**.
3. If you are prompted for a profile name, make the appropriate selection and click **OK**.

   Your email application opens with your key information already in place.
4. Address the message and send it.

Note: If this method doesn't work for you, you can open PGPkeys, select your keypair, pull down the Edit menu and select Copy, open an email message, then Paste. With some email applications you can simply drag your key from PGPkeys into the text of your email message to transfer the key information.

Exporting your public key to a file

Another method of distributing your public key is to copy it to a file and then make this file available to the person with whom you want to communicate.

There are three ways to export or save your public key to a file:

- Select the icon representing your keypair from PGPkeys, then choose **Export** from the **Keys** menu. Enter the name of the file to which you want to save the key.
- Drag the icon representing your keypair from PGPkeys to the folder where you want to save the key.
- Select the icon representing your keypair in PGPkeys, choose **Copy** from the **Edit** menu, then choose **Paste** to insert the key information into a text document.

Copy your public key from a smart card directly to someone's keyring

Another method of distributing your public key—if you have it on a smart card—is to copy it from the smart card directly to someone's keyring. For more information about how to do this, refer to "Copying a keypair from your keyring to a smart card" on page 71.

Obtaining the public keys of others

Just as you need to distribute your public key to those who want to send you encrypted mail or to verify your digital signature, you need to obtain the public keys of others so you can send them encrypted mail or verify their digital signatures.

There are three ways to obtain someone's public key:

- Get the key from a public keyserver
- Add the public key to your keyring directly from an email message
- Import the public key from an exported file

Public keys are just blocks of text, so they are easy to add to your keyring by importing them from a file or by copying them from an email message and then pasting them into your public keyring.

Getting public keys from a keyserver

If the person to whom you want to send encrypted mail is an experienced PGP user, it is likely that a copy of his or her public key is on a keyserver. This makes it very convenient for you to get a copy of the most up-to-date key whenever you want to send him or her mail and also relieves you from having to store a lot of keys on your public keyring.

If you are in a corporate setting, then your administrator may direct you to use a corporate key server that holds all of your organization's frequently used keys. In this case, your PGP software is probably already configured to access the appropriate server.

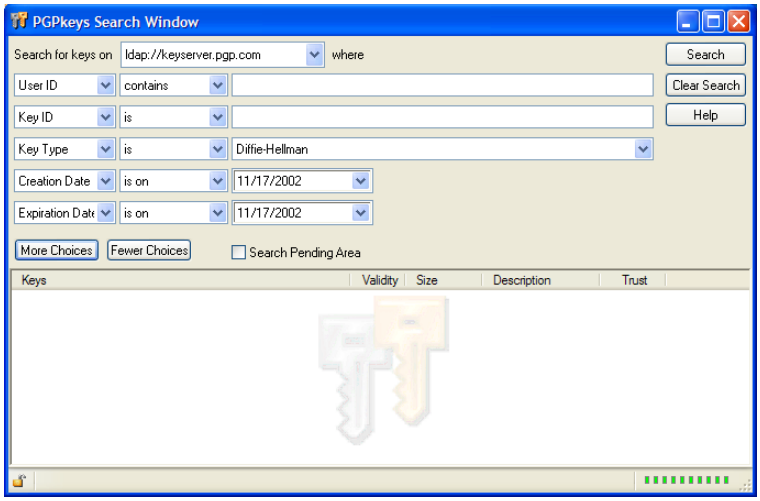
There are a number of public keyservers, such as the one maintained by PGP Corporation, where you can locate the keys of most PGP users. If the recipient has not pointed you to the Web address where his or her public key is stored, you can access any keyserver and do a search for the user's name or email address. This may or may not work, as not all public keyservers are regularly updated to include the keys stored on all the other servers.

To get someone's public key from a keyserver:

1. Open PGPkeys.

2. Choose **Search** from the **Server** menu or click the Search button in PGPkeys.

   The PGPkeys Search window appears.



3. Choose the server you wish to search from the Search for Keys On drop-down menu.
4. Specify your search criteria.

   You can search for keys on a key server by specifying values for multiple key characteristics.

   The inverse of most of these operations is also available. For example, you may search using "User ID is not Charles" as your criteria.
5. Enter the value you want to search for.
6. Click **More Choices** to add additional criteria to your search; for example, Key IDs with the name Taggert created on or before February 2, 1905.
7. To begin the search, click **Search**.

   A progress bar appears displaying the status of the search. To cancel a search in progress, click **Stop Search**.

   The results of the search appear in the window.
8. To import the keys, drag them to the PGPkeys main window.
9. Close the PGPkeys Search Window screen.

Getting public keys from email messages

A convenient way to get a copy of someone's public key is to have that person include it in an email message. When a public key is sent through email, it appears as a block of text in the body of the message.

To add a public key from an email message:

- If you have an email application that is supported by the PGP plug-ins, then click in your email application to extract the sender's public key from the email and add it to your public keyring.
- If you are using an email application that is not supported by the plug-ins, you can add the public key to the keyring by copying the block of text that represents the public key and pasting it into PGPkeys.

Importing keys and X.509 certificates

You can import PGP public keys and PKCS-12 X.509 certificates (a digital certificate format used by most Web browsers) to your PGP public keyring. You can also import Privacy Enhanced Mail (PEM) format X.509 certificates from your browser by copying and pasting into your public keyring. Another method for obtaining someone's public key is to have that person save it to a file from which you can import it or copy and paste it into your public keyring.

There are three methods of extracting someone's public key and adding it to your public keyring:

- Select **Import** from the **Keys** menu, and then navigate to the file where the public key is stored
- Drag the file containing the public key onto the main PGPkeys window
- Open the text document where the public key is stored, select the block of text representing the key, and then choose **Copy** from the **Edit** menu. In PGPkeys, choose **Paste** from the **Edit** menu to copy the key. The key then shows up as an icon in PGPkeys

You can also get PKCS-12 X.509 private keys by exporting them from your browser and dropping them into PGPkeys, or by choosing **Import** from the **Keys** menu.

Note: When importing an X.509 certificate, the certificate must be imported from a file with a .PEM, .PFX, or .P12 extension.

Validating keys

When you exchange keys with someone, it is sometimes hard to tell if the key really belongs to that person. PGP software provides a number of safeguards that allow you to check a key's authenticity and to certify that the key belongs to a particular owner (that is, to *validate* it). PGP warns you if you attempt to use a key that is not valid and also by default warns you when you are about to use a marginally valid key.

For more information on validity and trust, see *An Introduction to Cryptography*.

16 Managing Keys

This chapter explains how to examine and manage the keys stored on your keyrings.

The sections in this chapter are:

- The PGPkeys screen
- PGPkeys attribute definitions
- Specifying a default keypair on your PGP keyring
- Importing and exporting keys on your PGP keyring
- Deleting a key or signature on your PGP keyring
- Disabling and enabling keys on your PGP keyring
- Examining and setting key properties
- General key properties
- Subkeys properties
- Designated revoker properties
- Additional Decryption Key properties
- Adding an X.509 certificate to your PGP key
- Splitting and rejoining keys
- Updating your key on a keyserver
- Reconstructing your key

Overview

The keys you create, as well as those you collect from others, are stored on keyrings, which are essentially files stored on your hard drive or on a floppy disk. Normally your private keys are stored in a file named secring.skr and your public keys are stored in another file named pubring.pkr. These files are usually located in your PGP folder and can be viewed and edited from the PGPkeys window.

Note: As a result of your private key being encrypted automatically and your passphrase being uncompromised, there is little danger in leaving your keyrings on your computer. However, if you are not comfortable storing your keys in the default location, you can choose a different filename or location.

Occasionally, you may want to examine or change the attributes associated with your keys. For instance, when you obtain someone's public key, you might want to identify its type (either RSA or Diffie-Hellman/DSS), check its fingerprint, or determine its validity based on any digital signatures included with the key.

You may also want to sign someone's public key to indicate that you believe it is valid, assign a level of trust to the key's owner, or change a passphrase for your private key. You may even want to search a key server for someone's key

You perform all of these key-management functions from PGPkeys.

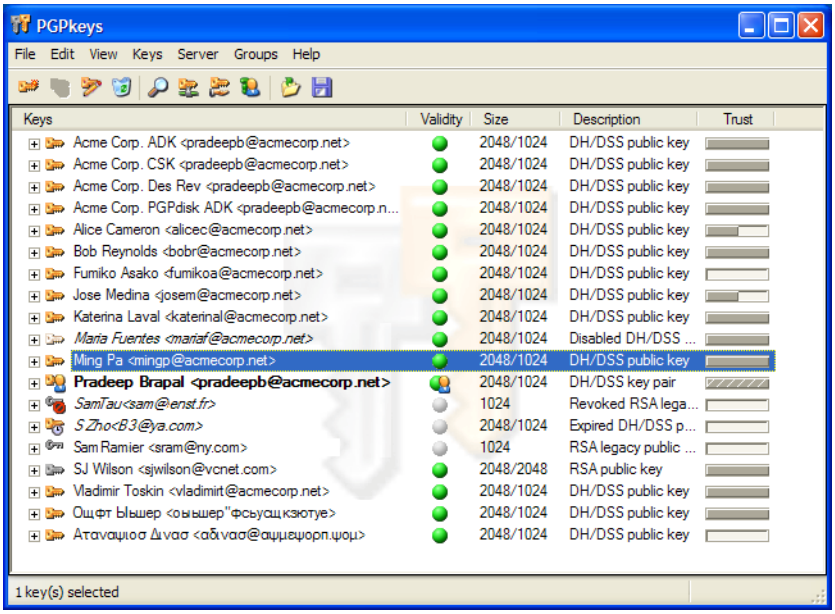
The PGPkeys screen

The PGPkeys screen displays the keys you have created for yourself, as well as any public keys you have added to your public keyring. It is from this window that you perform all your key management functions.

To open the PGPkeys screen:

- open the **Start** menu, click **Programs—>PGP—>PGPkeys**
- click the PGPtray lock icon ( ) in the System tray, and then click **PGPkeys**
- double-click the keys icon ( ) in the PGP program folder

The PGPkeys screen appears.



PGPkeys attribute definitions

Some of the attributes associated with keys can be displayed in the main PGPkeys window. You can choose which attributes you want to make visible by selecting them from the View menu. For each selected item in the View menu, PGPkeys displays a column in the main window. If you want to change the order of these columns, click and drag the header of the column you want to move.

For a list of PGPkeys attribute definitions, see the following table.

Attribute	Description
Keys	Shows an iconic representation of the key along with the user name, email address, photograph of the owner, and the names of the key's signers. A gold key and user represents your Diffie-Hellman/DSS keypair, which consists of your private key and your public key. A gray key and user represents an RSA keypair, which consists of your private key and your public key. A single gold key represents a Diffie-Hellman/DSS public key. A single gray key represents an RSA public key. When a key or keypair is dimmed, the keys are temporarily unavailable for encrypting and signing. You can disable a key from the PGPkeys window, which prevents seldom-used keys from cluttering up the Key Selection dialog box. A gray key on a gold card represents an RSA key stored on a smart card. Currently, the only key type supported on smart cards is RSA. A key with a red X indicates that the key has been revoked. Users revoke their keys when they are no longer valid or have been compromised in some way. A single key with a clock icon represents a public key or keypair that has expired. Two users represent a group email distribution list. Additional icons can be listed with a key indicating that a signature, certificate, or photographic user ID accompanies the key. A pencil or fountain pen indicates the signatures of the PGP users who have vouched for the authenticity of the key: - A signature with a red X through it indicates a revoked signature. - A signature with a dimmed pencil icon indicates a bad or invalid signature. - A signature with a blue arrow next to it indicates that it is exportable. A certificate represents an X.509 certificate, a recognized electronic document used to prove identity and public key ownership over a communication network. A clock indicates an expired X.509 certificate. A red X indicates a revoked X.509 certificate. This icon indicates that a photographic user ID accompanies the public key.

Attribute	Description
Validity	Indicates the level of confidence that the key actually belongs to the alleged owner. The validity is based on who has signed the key and how well you trust the signer(s) to vouch for the authenticity of a key. The public keys you sign yourself have the highest level of validity, based on the assumption that you only sign someone's key if you are totally convinced that it is valid. The validity of any other keys, which you have not personally signed, depends on the level of trust you have granted to any other users who have signed the key. If there are no signatures associated with the key, then it is not considered valid, and a message indicating this fact appears whenever you encrypt to the key. Validity is indicated by either circle or bar icons, depending upon your Advanced Options "Display marginal validity level" setting. If not enabled, then validity appears as: a gray circle for invalid keys and marginally valid keys if the Advanced Options "Treat marginally valid keys as invalid" is set a green circle for valid keys that you do not own a green circle and a user for valid keys that you own In a corporate environment, your PGP administrator may sign users' keys with the Corporate Signing Key. Keys signed with the Corporate Signing Key are usually assumed to be completely valid.
Size	Shows the number of bits used to construct the key. Generally, the larger the key, the less chance that it will ever be compromised. However, larger keys require slightly more time to encrypt and decrypt data than do smaller keys. When you create a Diffie-Hellman/DSS key, there is one number for the Diffie-Hellman portion and another number for the DSS portion. The DSS portion is used for signing, and the Diffie-Hellman portion for encryption. When you create an RSAv4 key, the first number represents the encryption key and the second number represents the signing key.
Description	Describes the type of information displayed in the Keys column: key type, type of ID, or signature type.
Additional Decryption Key	Shows whether the key has an associated Additional Decryption Key.
Key ID	A unique identifying number associated with each key. This identification number is useful for distinguishing between two keys that share the same user name and email address.

Attribute	Description
Trust	Indicates the level of trust you have granted to the owner of the key to serve as an introducer for the public keys of others. This trust comes into play when you are unable to verify the validity of someone's public key for yourself and instead rely on the judgment of other users who have signed the key. When you create a new keypair, these keys are considered implicitly trustworthy, as shown by the striping in the trust and validity bars, or by a green dot and user icon. An empty bar indicates an invalid key or an untrusted user. A half-filled bar indicates a marginally valid key or marginally trusted user. A striped bar indicates a valid key that you own and is implicitly trusted, regardless of the signatures on the key. A full bar indicates a completely valid key or a completely trusted user. When a public key on your keyring is signed by another user, the level of authenticity for that key is based on the trust you have granted to the signer. Use the Key Properties screen to assign the signer a level of trust: Trusted, Marginal, or Untrusted.
Expiration	Shows the date when the key will expire. Most keys are set to Never; however, there may be instances when the owner of a key wants it to be used for only a fixed period of time. A single key with a clock icon represents a public key or keypair that has expired.
Creation	Shows the date when the key was originally created. You can sometimes make an assumption about the validity of a key based on how long it has been in circulation. If the key has been in use for a while, it is less likely that someone will try to replace it because there are many other copies in circulation. Never rely on creation dates as the sole indicator of validity.

Specifying a default keypair on your PGP keyring

When encrypting messages or files, PGP gives you the option to additionally encrypt to a keypair that you specify as your default keypair. When you sign a message or someone's public key, PGP will use this keypair by default. Your default keypair is displayed in bold type to distinguish it from your other keys. If you have more than one keypair, you may want to specifically designate one pair as your default pair.

To specify your default keypair:

1. Open PGPkeys and highlight the keypair you want to designate as your default key.
2. Choose **Set Default** from the **Keys** menu.

   The selected keypair is displayed in bold type, indicating that it is now designated as your default keypair.

Importing and exporting keys on your PGP keyring

Although you often distribute your public key and obtain the public keys of others by cutting and pasting the raw text from a public or corporate key server, you can also exchange keys by importing and exporting them as separate text files.

For instance, someone could hand you a disk containing their public key, or you might want to make your public key available over an FTP server.

Deleting a key or signature on your PGP keyring

At some point you may want to remove a key or a signature from your PGP keyring. When you delete a key or signature from a key, it is removed and not recoverable. Signatures and user IDs can be re-added to a key, and an imported public key can be re-imported to your keyring. However, a private key that exists only on that keyring cannot be recreated, and all messages encrypted to its public key copies can no longer be decrypted.

Note: If you want to delete a signature or user ID associated with your public key on a key server, see "Updating your key on a keyserver" on page 141 for instructions.

To delete a key or signature from your PGP keyring:

1. Open PGPkeys and select the key or signature you want to delete.
2. Choose **Delete** from the **Edit** menu or click in the PGPkeys toolbar.

   The Confirmation screen appears.
3. Click **OK**.

Disabling and enabling keys on your PGP keyring

Sometimes you may want to temporarily disable a key, which can be useful when you want to retain a public key for future use, but you don't want it cluttering up your recipient list every time you send mail.

To disable a key:

1. Open PGPkeys and select the key you want to disable.
2. Select **Disable** in the **Keys** menu.

   The key is dimmed and is temporarily unavailable for use.

To enable a key:

1. Open PGPkeys and select the key you want to enable.
2. Select **Enable** in the **Keys** menu.

   The key becomes visible and can be used as before.

Examining and setting key properties

In addition to the general attributes shown in the PGPkeys window, you can also examine and change other key and subkey properties.

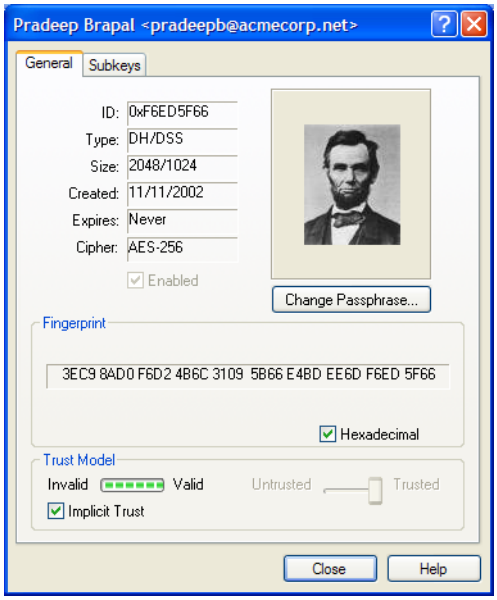
The Key Properties window includes the General, Subkeys, Revokers, and ADK tabs, each of which gives you necessary information about a person's public key, or the ability to create, configure, edit, or delete attributes in your own public key.

The following sections describe each element in more detail.

General key properties

From the General tabbed page, you can verify someone's public key using their key fingerprint, grant trust to a key, and change the passphrase on your own key as well as view other key attributes.

To access the General Key Properties panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu.



Verifying someone's public key

In the past it was difficult to know for certain whether a key belonged to a particular individual unless that person physically handed the key to you on a floppy disk. Exchanging keys in this manner is not usually practical, especially for users who are located many miles apart.

There are several ways to check a key's fingerprint, but the safest is to call the person and have them read the fingerprint to you over the phone. Unless the person is the target of an attack, it is highly unlikely that someone would be able to intercept this random call and imitate the person you expect to hear on the other end. You can also compare the fingerprint on your copy of someone's public key to the fingerprint on their original key on a public server.

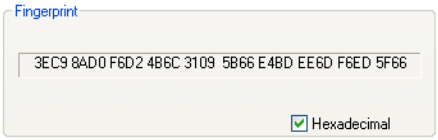
The fingerprint can be viewed in two ways: in a unique list of words or in its hexadecimal format.

To check a public key with its digital fingerprint:

1. Open PGPkeys and select the public key you want to verify.
2. Choose **Properties** from the **Keys** menu or click to open the Properties screen.

   The Properties screen opens.
3. Use the series of words or characters displayed in the Fingerprint text box to compare with the original fingerprint.

   By default, a word list is displayed in the **Fingerprint** text box. However, you can select the **Hexadecimal** check box to view the fingerprint in 20 hexadecimal characters.



Hexadecimal view

Word list view

The word list in the fingerprint text box is made up of special authentication words that PGP uses and are carefully selected to be phonetically distinct and easy to understand without phonetic ambiguity.

The word list serves a similar purpose as the military alphabet, which allows pilots to convey information distinctly over a noisy radio channel. If you'd like to know more about the word hash technique and view the word list, see Appendix C, Biometric Word Lists.

Signing someone's public key

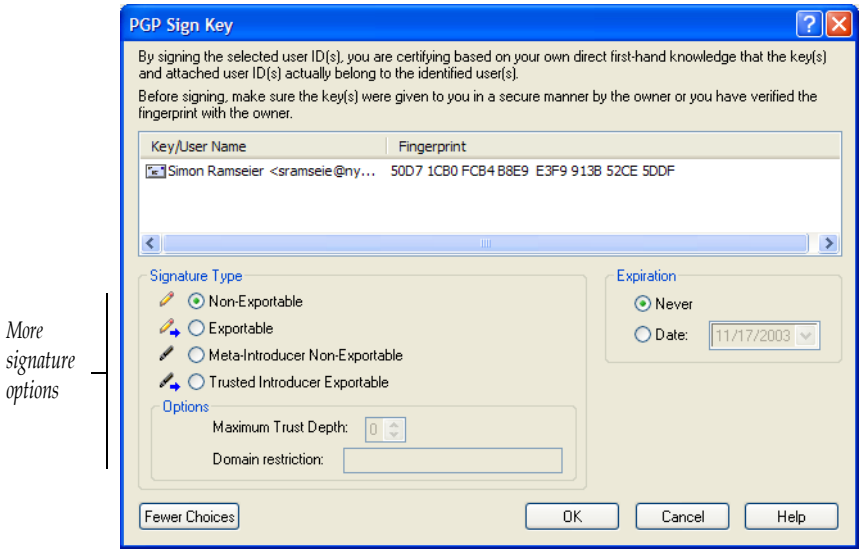
When you create a keypair, the keys are automatically signed by themselves. Similarly, once you are sure that a key belongs to the proper individual, you can sign that person's public key, indicating that you are sure it is a valid key. When you sign someone's public key, a signature icon along with your user name is shown attached to that key.

To sign someone's public key:

1. Open PGPkeys and select the public key which you want to sign.
2. Choose **Sign** from the **Keys** menu or click to open the Sign Keys screen.

   The Sign Keys screen appears with the public key and fingerprint displayed in the text box.
3. Click the **Allow signature to be Exported** check box, to allow your signature to be exported with this key.

   An exportable signature is one that is allowed to be sent to servers and travels with the key whenever it is exported, such as by dragging it to an email message. The check box provides a shorthand means of indicating that you wish to export your signature.
4. Click the **More Choices** button to configure options such as signature type and signature expiration.


PGP Sign Key
By signing the selected user ID(s), you are certifying based on your own direct first-hand knowledge that the key(s) and attached user ID(s) actually belong to the identified user(s).
Before signing, make sure the key(s) were given to you in a secure manner by the owner or you have verified the fingerprint with the owner.
Key/User Name
Fingerprint
Simon Ramseier <sramseie@ny...
50D7 1CB0 FCB4 B8E9 E3F9 913B 52CE 5DDF
Signature Type
Non-Exportable
Exportable
Meta-Introducer Non-Exportable
Trusted Introducer Exportable
Options
Maximum Trust Depth:
Domain restriction:
Expiration
Never
Date:
11/17/2003
Fewer Choices
OK
Cancel
Help
More signature options

Choose a signature type to sign the public key with. Your choices are:

– **Non-exportable.** Use this signature when you believe the key is valid, but you don't want others to rely on your certification. This signature type cannot be sent with the associated key to a key server or exported in any way.

- **Exportable.** Use exportable signatures in situations where your signature is sent with the key to the key server, so that others can rely on your signature and trust your keys as a result. This is equivalent to checking the Allow signature to be exported check box on the **Sign Keys** menu.
- **Meta-Introducer Non-Exportable**. Certifies that this key and any keys signed by this key with a Trusted Introducer Validity Assertion are fully trusted introducers to you. This signature type is non-exportable.
- The **Maximum Trust Depth** option enables you to identify how many levels deep you can nest trusted-introducers. For example, if you set this to 1, there can only be one layer of introducers below the meta-introducer key.
- **Trusted Introducer Exportable.** Use this signature in situations where you certify that this key is valid, and that the owner of the key should be completely trusted to vouch for other keys. This signature type is exportable. You can restrict the validation capabilities of the trusted introducer to a particular email domain.

5. If you want to limit the Trusted Introducer's key validation capabilities to a single domain, enter the domain name in the Domain Restriction text box.
6. If you want to assign an expiration date to this signature, enter the date on which you want this signature to expire in the Date text box. Otherwise, the signature will never expire.
7. Click **OK**.
8. Enter your passphrase, then click **OK**.

   An icon associated with your user name is now included with the public key that you just signed.

Granting trust for key validations

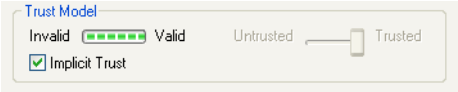
Besides certifying that a key belongs to someone, you can assign a level of trust to the owner of the keys indicating how well you trust them to act as an introducer for others, whose keys you may get in the future. This means that if you ever get a key from someone that has been signed by an individual whom you have designated as trustworthy, the key is considered valid even though you have not done the check yourself.

To grant trust for a key:

1. Open PGPkeys and select the key for which you want to change the trust level.

Note: You must sign the key before you can set the trust level for it.

2. Choose **Properties** from the **Keys** menu or click to open the Properties screen.
3. Use the Trust Level sliding bar to choose the appropriate level of trust for the key-pair.



4. Close the dialog box to accept the new setting.

Changing your passphrase

It's a good practice to change your passphrase at regular intervals, perhaps every three months. More importantly, you should change your passphrase the moment you think it has been compromised, for example, by someone looking over your shoulder as you typed it in.

To change your passphrase:

1. Open PGPkeys and select the key for which you want to change the passphrase.

   Choose **Properties** from the **Keys** menu or click to open the Properties screen.

   The Properties screen appears.
2. Click **Change Passphrase** from the **General** tab.

   The Passphrase screen appears.

Note: If you want to change the passphrase for a split key, you must first rejoin the key shares. Click **Join** to collect the key shares.

3. Enter your current passphrase in the space provided, then click **OK**.

   The Confirmed Passphrase screen appears.
4. Enter your new passphrase in the first text box. Press **Tab** to advance to the next text box and confirm your entry by entering your new passphrase again.
5. Click **OK**.

Caution: If you are changing your passphrase because you feel that your passphrase has been compromised, you should wipe all backup keyrings and wipe your freespace.

Adding a new user name or address to your keypair

You may have more than one user name or email address for which you want to use the same keypair. After creating a keypair, you can add alternate names and addresses to the keys. You can only add a new user name or email address if you have both the private and public keys.

To add a new user name or address to your key:

1. Open PGPkeys and select the keypair for which you want to add another user name or address.
2. Choose **Add/Name** from the **Keys** menu.

   The PGP New User Name screen appears.
3. Enter the new name and email address in the appropriate fields, then click **OK**.

   The PGP Enter Passphrase screen appears.
4. Enter your passphrase, then click **OK**.

   The new name is added to the end of the user name list associated with the key. If you want to set the new user name and address as the primary identifier for your key, select the name and address and then choose **Set as Primary Name** from the **Keys** menu.

Note: When you add or change information in your keypair, always update it on the key server so that your most current key can be available to anyone.

Adding a photographic ID to your key

You can include a photographic user ID with your PGP keys.

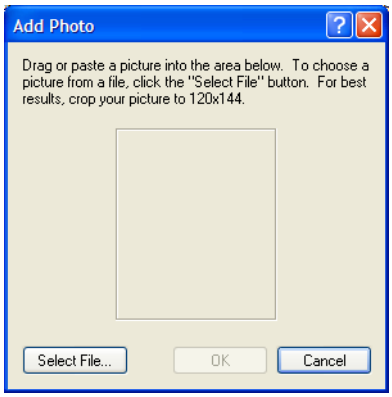
This feature is available for Diffie-Hellman/DSS and RSA keys. The Photographic ID feature is not supported by RSA Legacy keys.

Caution: Although you can view the photographic ID accompanied with someone's key for verification, you should always check and compare the digital fingerprints.

To add your photograph to your key:

1. Open PGPkeys and select your keypair and then click **Add Photo** on the **Keys** menu.

The Add Photo screen opens.


Add Photo
Drag or paste a picture into the area below. To choose a picture from a file, click the "Select File" button. For best results, crop your picture to 120x144.
Select File...
OK
Cancel

2. Drag or paste your photograph onto the Add Photo screen or browse to it by clicking **Select File**.

Note: The photograph can be from the Clipboard, a .JPG, or .BMP file. For maximum picture quality, crop the picture to 120 x 144 pixels before adding it to the Add Photo screen. If you do not do this, PGP will scale the picture for you.

3. Click **OK**.

   The **Passphrase** dialog box opens.

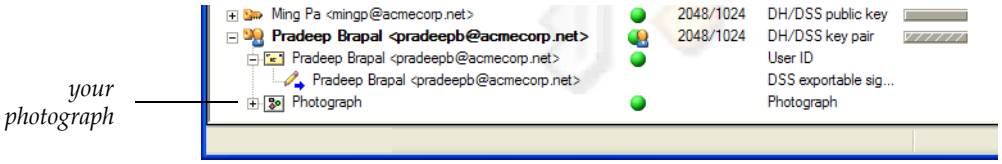
4. Enter your passphrase in the space provided, then click **OK**.

   Your photographic user ID is added to your public key and is listed in the PGPkeys window.

Note: When you add or change information in your keypair always update it on the key server so that your most current key can be available to anyone.

To replace your photographic ID:

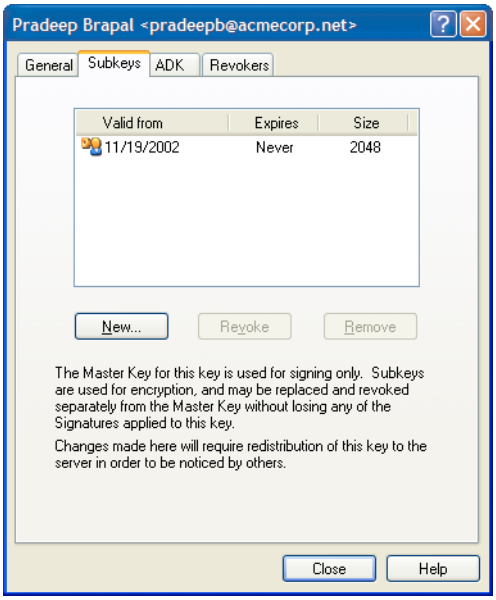
1. Open PGPkeys and select the photograph which is listed under your key.



2. Choose **Delete** from the **Edit** menu.
3. Add your new photographic ID using the instructions outlined in "Adding a photographic ID to your key" on page 125.

Subkeys properties

To access the Subkeys Properties panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The Key Properties screen appears. Click the **Subkeys** tab. The Subkeys panel appears.


Pradeep Brapal <pradeepb@acmecorp.net>
General
Subkeys
ADK
Revokers
Valid from
Expires
Size
11/19/2002
Never
2048
New...
Revoke
Remove
The Master Key for this key is used for signing only. Subkeys are used for encryption, and may be replaced and revoked separately from the Master Key without losing any of the Signatures applied to this key.
Changes made here will require redistribution of this key to the server in order to be noticed by others.
Close
Help

Creating new subkeys

Every Diffie-Hellman/DSS and RSA key is actually two keys: a signing key and an encryption subkey. PGP Version 6.0 and above provides the ability to create and revoke new encryption keys without sacrificing your master signing key and the signatures collected on it.

One of the most common uses for this feature is to create multiple subkeys that are set to be used during different periods of the key's lifetime. For example, if you create a key that will expire in three years, you might also create three subkeys and use each of them for one of the years in the lifetime of the key. This can be a useful security measure and provides an automatic way to periodically switch to a new encryption key without having to recreate and distribute a new public key.

This feature is available for Diffie-Hellman/DSS and RSA keys. Subkeys are not supported by RSA Legacy keys.

To create new subkeys:

1. Open PGPkeys and select your keypair, then click **Properties** from the **Keys** menu or click .

   The Properties screen appears.

2. Click the **Subkeys** tab.

   The Subkeys screen appears.

3. To create a new subkey, click **New**.

   The New Subkey screen opens.

4. Enter a key size from 1024 to 3072 bits, or enter a custom key size from 1024 to 4096 bits.

5. Indicate the start date on which you want your subkey to activate.

6. Indicate when you want your subkey to expire. You can either use the default selection, which is Never, or you can enter a specific date after which the subkey will expire.

Note: To avoid confusion when maintaining more than one subkey on your keypair, try not to overlap your subkeys start and expiration dates.

7. Click **OK**.

   The Passphrase screen appears.

8. Enter your passphrase and then click **OK**.

   Your new subkey is listed in the Subkey window.

Note: When you add or change information in your keypair, always update it on the key server so that your most current key can be available to anyone.

Revoking subkeys

To revoke a subkey:

1. Open PGPkeys and select your keypair, then click **Properties** from the **Keys** menu or click .

   The Properties screen appears.

2. Click the **Subkeys** tab.

   The Subkeys screen opens.

3. Select the subkey, and click **Revoke**.

   A PGP Warning appears informing you that once you revoke the subkey, other user's will not be able to encrypt data to it.

4. Click **Yes** to revoke the subkey or click **No** to cancel this operation.

   The Passphrase screen appears.

5. Enter your passphrase, then click **OK**.

   The subkey is revoked and the icon changes to a key with a red X.

Removing subkeys

To remove a subkey:

1. Open PGPkeys and select your keypair, then click **Properties** from the **Keys** menu, or click .

   The Properties screen appears.

2. Click the **Subkeys** tab.

   The Subkeys screen opens.

3. Select the subkey, and click **Remove**.

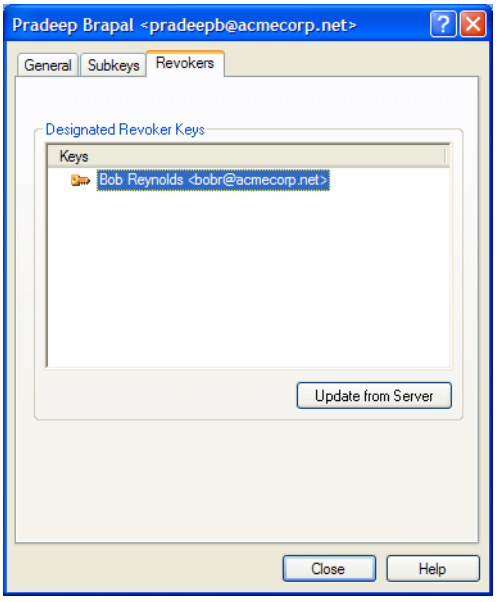
   A PGP Warning appears informing you that once you remove the subkey, you will not be able to decrypt information encrypted to it.

4. Click **Yes** to remove the subkey or click **No** to cancel this operation.

   The subkey is removed and the key disappears from the subkeys window.

Designated revoker properties

To access the Revokers panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The Key Properties screen appears. Click the **Revokers** tab. The Revokers panel appears. (If there are no designated revokers for the selected key, then the Revokers tab does not appear.)



The Revokers panel lists any keys that have the ability to revoke your PGP key, and provides a convenient means for updating a revokers' key with the Update from Server button.

If the key belonging to the revoker is not on your keyring, then "*Unknown Key*" followed by the keys' key ID displays instead of the user ID. Highlight the key ID, and click the **Update from Server** button to search for the key on a key server.

Appointing a designated revoker

It is possible that you might forget your passphrase someday or lose your private key (your laptop is stolen or your hard drive crashes, for example). Unless you are also using Key Reconstruction and can reconstruct your private key, you would be unable to use your key again, and you would have no way of revoking it to show others not to encrypt to it. To safeguard against this possibility, you can appoint a third-party key revoker. The third-party you designate is then able to revoke your key just as if you had revoked it yourself.

Note: For a key to appear revoked to another user, both the revoked key and the Designated Revoker key must be on his/her keyring. Thus, the designated revoker feature is most effective in a corporate setting, where all users' keyrings contain the company's Designated Revoker key. If the revokers' key is not present on a person's keyring, then the revoked key does not appear revoked to that user and he/she may continue to encrypt to it.

This feature is available for Diffie-Hellman/DSS and RSA keys. Designated revokers are not supported by RSA Legacy keys.

To add a designated revoker to your key:

1. Open PGPkeys and then select the keypair for which you want to add a revoker.
2. Select **Add/Revoker** from the **Keys** menu.

   A screen opens and displays a list of keys.
3. Select the key(s) in the User ID list that you want to appoint as a revoker.
4. Click **OK**.

   A confirmation screen appears.
5. Click **OK** to continue.

   The Passphrase screen appears.
6. Enter your passphrase, then click **OK**.
7. The selected key(s) is now authorized to revoke your key. For effective key management, distribute a current copy of your key to the revoker(s) or upload your key to the server.

Revoking a key

If the situation ever arises that you no longer trust your personal keypair, you can issue a revocation to the world telling everyone to stop using your public key. The best way to circulate a revoked key is to place it on a public key server.

To revoke a key:

1. Open PGPkeys and select the keypair you want to revoke.
2. Choose **Revoke** from the **Keys menu**.

   The Revocation Confirmation screen appears.
3. Click **OK** to confirm your intent to revoke the selected key.

   The PGP Enter Passphrase screen appears.
4. Enter your passphrase, then click **OK**.

   When you revoke a key, it is marked out with a red X to indicate that it is no longer valid.
5. Send the revoked key to the server so everyone will know not to use your old key.

Additional Decryption Key properties

To access the ADK panel for a particular key, select the desired key and then choose **Properties** from the **Keys** menu. The Key Properties screen appears. Click the **ADK** tab. The ADK panel appears. (Note, if there are no Additional Decryption Keys associated with the selected key, then the ADK tab does not appear.)

The ADK panel lists all Additional Decryption Keys (ADKs) for the selected key. ADKs are keys that allow the security officers of an organization to decrypt messages that have been sent to or from people within your organization. There are two types of keys: incoming additional decryption keys and outgoing additional decryption keys.

Note: Although your PGP administrator should not ordinarily use the Additional Decryption keys, there may be circumstances when it is necessary to recover someone's email. For example, if someone is injured and out of work for some time or if email records are subpoenaed by a law enforcement agency and the corporation must decrypt mail as evidence for a court case.

Adding an X.509 certificate to your PGP key

The instructions in this section describe how to add an X.509 certificate to your keypair if you are using the iPlanet CMS Server. This process varies between Certificate Authorities and some of the terminology you must use when interacting with your CA is a policy decision. You may need to consult your company's PGP or PKI administrator for instructions.

An X.509 digital certificate is a recognized electronic document used to prove identity and public key ownership over a communication network.

You can request an X.509 digital certificate and add it to your keypair using PGP menu options and your company's Certificate Authority (CA) or a public CA (for example, VeriSign).

There are four main steps to adding an X.509 certificate to your keypair:

1. Retrieve the Root CA certificate from the CA and add it to your PGP keyring.
2. Enter information about the CA in the **CA** tab on the **Options** screen.
3. Request a certificate from the CA. Your X.509 certificate request is verified and signed by the CA.

   (The CA's signature on the certificate makes it possible to detect any subsequent tampering with the identifying information or the public key, and it implies that the CA considers the information in the certificate valid.)
4. Retrieve the certificate issued by the CA and add it to your keypair.

Each of these four steps is described in greater detail in the following sections.

To add an X.509 certificate to your PGP keypair:

1. Obtain and add the Root CA certificate to your PGP keyring.

   To do this, follow these steps:

   a. Open your Web browser and connect to the CA's enrollment site. If you do not know the URL, consult your company's PGP or PKI administrator.

   b. Locate and examine the Root CA certificate. This process varies between Certificate Authorities. For example, if your company were using the iPlanet CMS server, you would click the **Download a CA Certificate link**, and then click the **Examine this Certificate** button.

   c. Copy the key block for the Root CA certificate and paste it into your PGPkeys window.

      The Import Key screen appears and imports the Root CA certificate into your keyring.

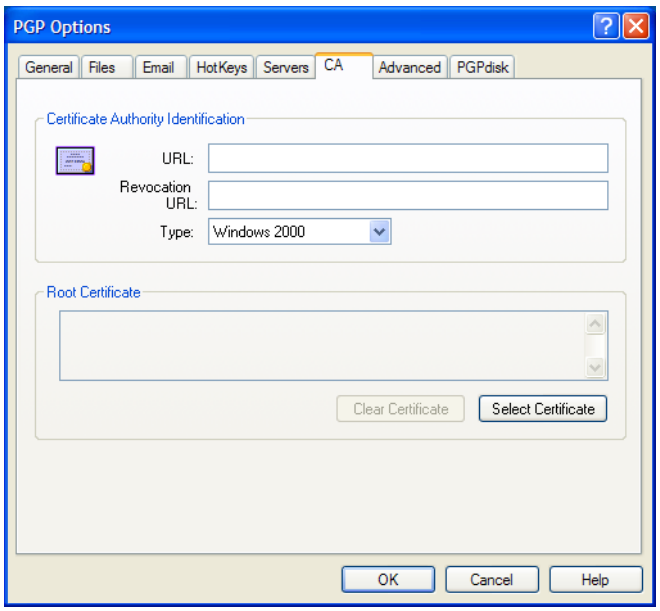
   d. Sign the Root CA certificate with your key to make it valid, then open the Key Properties and set the trust level. Trust must be set on the Root CA.

2. Configure the CA tab in the Options screen.

   To do this, follow these steps:

   a. Select **Options** from the PGPkeys **Edit** menu, then select the **CA** tab.

      The CA tab appears.



   b. Enter the CA's URL in the Certificate Authority Identification URL field, for example, https://nnn.nnn.nnn.nnn:nnnnn (this is the same URL you used to retrieve the Root CA).

   c. If there is a separate URL for retrieving certificate revocation lists (CRLs), enter it in the corresponding field.

      If you do not know the URL for Revocation, leave this field blank or consult your company's PGP or PKI administrator.

   d. In the Type box, specify the name of certificate authority you are using. Your choices are:

      Net Tools PKI

      VeriSign OnSite

      Entrust

      iPlanet CMS

      Windows 2000

   e. Click the **Select Certificate** button, then select the Root CA certificate you just retrieved.

The Root Certificate text box displays information on the selected root CA certificate. The terminology for the certificate is a policy decision. Typically, the following terminology is true for X.509 certificates.

Term:	Description:
CN (Common Name)	Often a description of the type of certificate (for example, "Root").
EMAIL	The email address for the certificate holder.
OU (Organizational Unit)	The organization to which the certificate belongs (for example, "Accounting").
O (Organization)	Typically the name of the company to which the certificate belongs (for example, "Secure Corp.").
L (Locality)	The location of the holder of the certificate (for example, "Santa Clara").

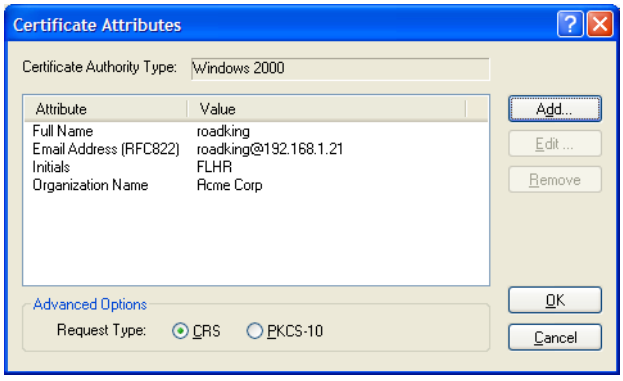
f. Click **OK**.

3. Make a certificate request.

   To do this, follow these steps:

   a. Right-click on your PGP keypair and select **Keys—>Add—>Certificate** from the **Keys** right-click menu.

      The Certificate Attributes dialog box appears.



   b. Verify the certificate attributes; use the **Add**, **Edit**, and **Remove** buttons to make any required changes, and click **OK**. The PGP Enter Passphrase screen appears.

   c. Enter the passphrase for your keypair, then click **OK**.

      The PGP Server Progress bar appears.

      The certificate request is sent to the CA server. The server authenticates itself to your computer and accepts your request.

In a corporate setting, your company's PGP or PKI administrator verifies your information in the request. The identifying information and public key are assembled and then digitally signed with the CA's own certificate to create your new certificate.

The administrator sends you an email message stating that your certificate is ready for retrieval.

4. Retrieve your certificate and add it to your keypair.

   In a corporate setting, your certificate may be retrieved and added to your keypair automatically depending on the settings your administrator has configured.

   If you do not have automatic certificate retrieval configured, you can retrieve your certificate and add it to your keyring manually. To do this, follow these steps:

   a. In PGPkeys, select the PGP key for which you made the certificate request.

   b. On the **Server** menu, select **Retrieve Certificate**.

      PGP contacts the CA server and automatically retrieves your new X.509 certificate and adds it to your PGP key.

Note: When you add or change information in your keypair, always update it on the key server so that your most current key can be available to anyone.

Splitting and rejoining keys

Any private key can be split into shares among multiple "shareholders" using a cryptographic process known as Blakely-Shamir key splitting. This technique is recommended for extremely high security keys. For example, PGP Corporation keeps a corporate key split between multiple individuals. Whenever we need to sign with that key, the shares of the key are rejoined temporarily.

Note: Split keys are not compatible with versions of PGP previous to 6.0.

Creating a split key

To split a key, select the keypair to be split and choose **Share Split** from the **Keys** menu. You are then asked to set up how many different shares will be required to rejoin the key. The shares are saved as files either encrypted to the public key of a

shareholder or encrypted conventionally if the shareholder has no public key. After the key has been split, attempting to sign with it or decrypt with it will automatically attempt to rejoin the key.

Note: You cannot split a key generated on a smart card because the private portion of your keypair is non-exportable.

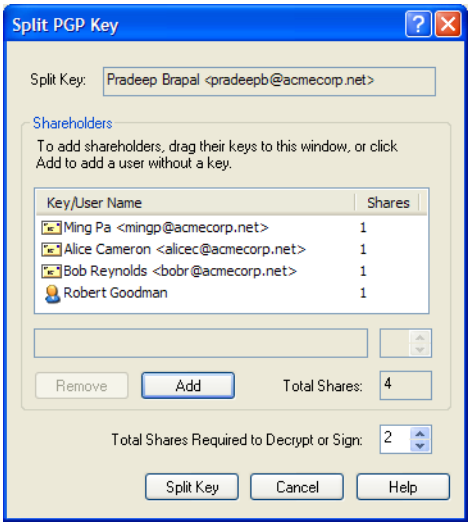
To create a split key with multiple shares:

1. In PGPkeys, create a new keypair or select an existing keypair that you want to split.
2. On the **Keys** menu, click **Share Split**.

   The Share Split screen opens.
3. Add shareholders to the keypair by dragging their keys from PGPkeys to the **Shareholder** list on the **Share Split** screen.

   To add a shareholder that does not have a public key, click **Add** on the Share Split screen, enter the persons name and then allow the person to type in their pass-phrase.
4. When all of the shareholders are listed, you can specify the number of key shares that are necessary to decrypt or sign with this key.

   The total number of shares that make up the Group Key in the following example is four and the total number of shares required to decrypt or sign is three. This provides a buffer in the event that one of the shareholders is unable to provide his or her key share or forgets the passphrase.



By default, each shareholder is responsible for one share. To increase the number of shares a shareholder possesses, click the name in the shareholder's list to display it in the text field below. Type the new number of key shares or use the arrows to select a new amount.

5. Click **Split Key**.

   A screen appears and prompts you to select a directory in which to store the shares.

6. Select a location to store the key shares.

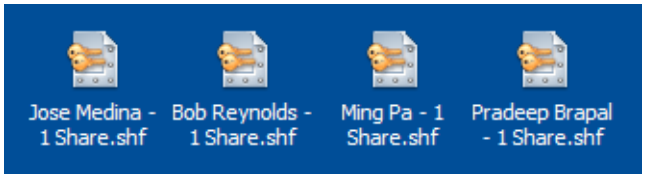
   The Passphrase screen appears.

7. Enter the passphrase for the key you want to split and then click **OK**.

   A confirmation dialog box opens.

8. Click **Yes** to split the key.

   The key is split and the shares are saved in the location you specified. Each key share is saved with the shareholder's name as the file name and a .shf extension, as shown in the example below:



9. Distribute the key shares to the owners, then delete the local copies.

   Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP to automatically attempt to rejoin the key.

Rejoining split keys

Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP to automatically attempt to rejoin the key. There are two ways to rejoin the key, locally and remotely.

Rejoining key shares locally requires the shareholders presence at the rejoining computer. Each shareholder is required to enter the passphrase for their key share.

Rejoining key shares remotely requires the remote shareholders to authenticate and decrypt their keys before sending them over the network. PGP's Transport Layer Security (TLS) provides a secure link to transmit key shares which allows multiple individuals in distant locations to securely sign or decrypt with their key share.

Caution: Before receiving key shares over the network, you should verify each shareholder's fingerprint and sign their public key to ensure that their authenticating key is legitimate.

To rejoin a split key:

1. Contact each shareholder of the split key. To rejoin key shares locally, the shareholders of the key must be present.

   To collect key shares over the network, ensure that the remote shareholders have PGP installed and are prepared to send their key share file. Remote shareholders must have:

   – their key share files and passwords

   – a keypair (for authentication to the computer that is collecting the key shares)

   – a network connection

   – the IP address or Domain Name of the computer that is collecting the key shares

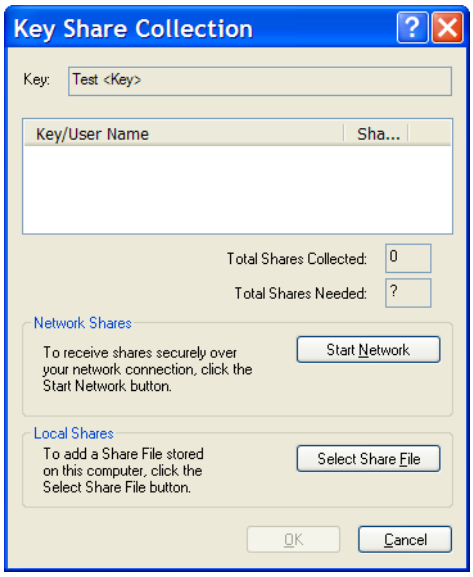
2. At the rejoining computer, use Windows Explorer to select the file(s) that you want to sign or decrypt with the split key.

3. Right-click on the file(s) and select **Sign or Decrypt** from the **PGP** menu.

   The PGP Enter Passphrase for Selected Key screen appears with the split key selected.

4. Click **OK** to reconstitute the selected key.

The Key Share Collection screen appears.



5. Do one of the following:

   – If you are collecting the key shares locally, click **Select Share File** and then locate the share files associated with the split key. The share files can be collected from the hard drive, a floppy disk, or a mounted drive. Continue with Step 6.

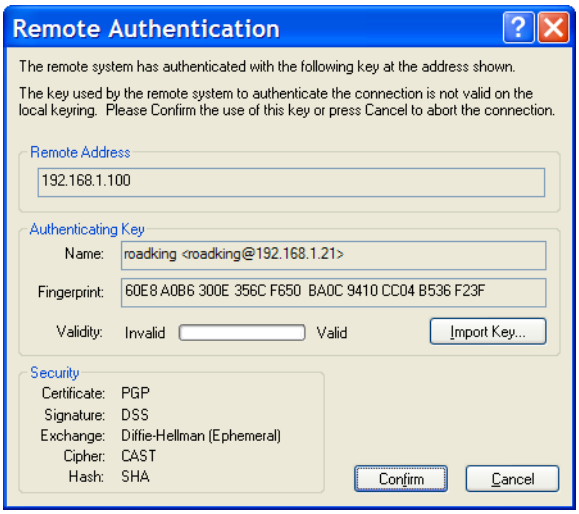
   – If you are collecting key shares over the network, click **Start Network**.

     The Passphrase dialog box opens. In the Signing Key box, select the keypair that you want to use for authentication to the remote system and enter the passphrase. Click **OK** to prepare the computer to receive the key shares.

     The status of the transaction is displayed in the Network Shares box. When the status changes to "Listening," the PGP application is ready to receive the key shares.

     At this time, the shareholders must send their key shares.

When a share is received, the Remote Authentication screen appears.


Remote Authentication
The remote system has authenticated with the following key at the address shown.
The key used by the remote system to authenticate the connection is not valid on the local keyring. Please Confirm the use of this key or press Cancel to abort the connection.
Remote Address
192.168.1.100
Authenticating Key
Name: roadking <roadking@192.168.1.21>
Fingerprint: 60E8 A0B6 300E 356C F650 BA0C 9410 CC04 B536 F23F
Validity: Invalid Valid
Import Key...
Security
Certificate: PGP
Signature: DSS
Exchange: Diffie-Hellman (Ephemeral)
Cipher: CAST
Hash: SHA
Confirm
Cancel

If you have not signed the key that is being used to authenticate the remote system, the key will be considered invalid. Although you can rejoin the split key with an invalid authenticating key, it is not recommended. You should verify each shareholder's fingerprint and sign each shareholder's public key to ensure that the authenticating key is legitimate.

6. Click **Confirm** to accept the share file.
7. Continue collecting key shares until the value for Total Shares Collected matches the value for Total Shares Needed on the Key Shares Collection screen.
8. Click **OK**.

   The file is signed or decrypted with the split key.

To send your key share over the network:

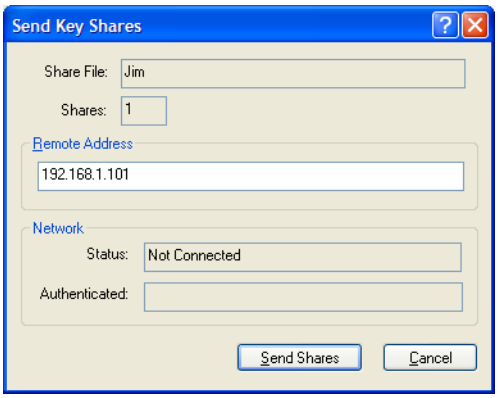
1. When you are contacted by the person who is rejoining the split key, make sure that you have these items:
   - your key share file and password
   - your keypair (for authentication to the computer that is collecting the key shares)
   - a network connection
   - the IP address or Domain Name of the rejoining computer collecting the key shares
2. Select **Send Key Shares** on the PGPkeys **File** menu.
3. Choose **Send Share File** from the PGPkeys **File** menu.

   The Select Share File screen appears.
4. Locate your key share and then click **Open**.

The PGP Enter Passphrase screen appears.

5. Enter your passphrase and then click **OK**.

   The Send Key Shares screen appears.



6. Enter the IP address or the Domain Name of the rejoining computer in the **Remote Address** text box, then click **Send Shares**.

   The status of the transaction is displayed in the **Network Status** box. When the status changes to "Connected," you are asked to authenticate yourself to the rejoining computer.

   The Remote Authentication screen appears asking you to confirm that the remote computer is the one to whom you want to send your key share.

7. Click **Confirm** to complete the transaction.

   After the remote computer receives your key shares and confirms the transaction, a message box appears stating that the shares were successfully sent.

8. Click **OK**.

9. Click **Done** in the Key Shares window when you have completed sending your key share.

Updating your key on a keyserver

If you ever need to change your email address, or if you acquire new signatures, all you have to do to replace your old key is send a new copy to the server; the information is automatically updated. However, you should keep in mind that public key servers are only capable of adding new information and will not allow removal of user names or signatures from your key.

If your key is ever compromised, you can revoke it; this tells the world to no longer trust that version of your key.

Removing signatures or user names associated with your key

At some point you may want to remove a subkey, a signature, or a user ID associated with a particular key.

Public keyservers are only capable of adding new information and will not allow removal of user names or signatures from your key. To remove signatures or user names associated with your public key, you must first remove your key from the server, make the required change, then post your key back on the server.

If your Server settings on the Options screen are configured to synchronize keys with the key server when you add names/photos/revokers to your key, your key is automatically updated on the server. If, however, your keys do not automatically synchronize with the server, follow the instructions outlined below to manually update your key on the key server.

Note: When you delete a key, signature, or user name from a key, it is removed and not recoverable. Signatures and user names can be added again to a key, and an imported public key can be imported again to your keyring. However, a private key that exists only on that keyring cannot be created again, and all messages encrypted to its public key copies can no longer be decrypted.

To remove signatures or user names from your key on a keyserver:

Note: This procedure is for removing signatures or user names associated with your key on LDAP key servers only. Additionally, the key server must be configured to allow this action. If you do not know the type server or its configuration settings, consult the key server administrator for your company before updating your key.

1. Open PGPkeys.
2. Choose **Search** from the **Server** menu or click in the PGPkeys menu.

   The PGPkeys Search window appears.
3. Choose the server you want to search from the Search for Keys On menu.
4. Specify your search criteria to locate your public key:

   The default is User ID, but you can click the arrows to select Key ID, Key Status, Key Type, Key Size, Creation Date, or Expiration Date. For example, you might search for all keys with the User ID of Fred.
5. To begin the search, click **Search**.

   The results of the search appear in the window.
6. Right-click on the key that you want to remove from the server, then select **Delete** from the menu.

The Passphrase screen appears.

7. Enter the passphrase for the key you want to remove from the server, then click **OK**.

   The Confirmation screen appears and the key is removed.

8. Update your key (remove the unwanted signatures or user names).
9. Copy the updated key to the server.

   If the key server is configured to synchronize keys with other key servers, your key will be updated on the other servers automatically upon synchronization.

Caution: If you delete your key from a key server, you should be aware that someone who has your public key on their keyring can upload it to the server again. You should check the server periodically to see if the key has reappeared—you may have to delete your key from the server more than once.

Reconstructing your key

If you ever lose your private key or you forget your passphrase, there is no way to recover from it unless your administrator has set up a key reconstruction policy, which includes setting up a key reconstitution server and enabling this feature in your PGP software. If this feature is enabled in your software, you would have provided recovery information—five secret questions and answers—and would have sent your key to the key reconstruction server.

If you sent your key to a reconstruction server, you can restore your keypair at any time as long as you have your public key and can answer at least three of the five secret questions you created.

To reconstruct your key from your company's reconstruction server:

1. Open PGPkeys, then select the key that you want to reconstruct.
2. Select **Reconstruct Key** from the **Key** menu.

   If the reconstruction server is a PGP key server, the Server User ID and Password screen appears. Enter your user ID and password to log on to the server. If you do not know your user ID or password, consult your administrator.

3. Click **OK**.

   The Key Reconstruction screen appears.

4. In the Key Reconstruction screen, enter answers in the Answer boxes to their corresponding questions. Keep in mind that your answers are case sensitive. You must be able to answer at least three questions to restore your key.

   You can use the Hide Answers check box to view or hide your answers.

5. Click **OK** to continue.

   The PGP Enter Confirmed Passphrase screen appears.

6. In the Passphrase box, enter a new string of characters or words you want to use as the new passphrase for your new keypair.

Note: Your passphrase should contain multiple words and may include spaces, numbers, and punctuation characters. Choose something that you can remember easily but that others won't be able to guess. The passphrase is case sensitive, meaning that it distinguishes between uppercase and lowercase letters. The longer your passphrase, and the greater the variety of characters it contains, the more secure it is. Strong passphrases include upper and lowercase letters, numbers, punctuation, and spaces but are more likely to be forgotten.

   To confirm your entry, press the TAB key to advance to the next line, then enter the same passphrase again.

7. Click **OK**.

   Your keypair is reconstituted and appears in PGPkeys.

A Setting PGP Options

This chapter describes how to set PGP options to suit your particular computing environment.

About PGP Options

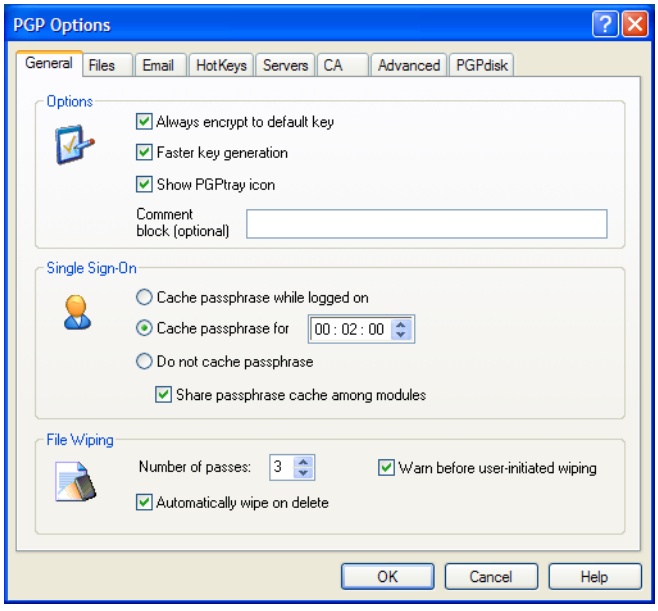
PGP is configured to accommodate the needs of most users, but you have the option of adjusting settings to suit your requirements. You specify these settings on the PGP Options screen.

To access the PGP Options screen, do either of the following:

- Click the PGP icon in the System Tray (called the PGPtray icon) and select **Options** from the menu.
- Open PGP Keys, pull down the Edit menu, and select **Options**.

Setting General options

Use the General tab to specify optional, single sign-on, and file wiping settings.



Make your selections for the following options:

- **Always Encrypt to Default Key**. When this setting is selected, all the email messages and file attachments you encrypt with a recipient's public key are also encrypted to you using your default public key. It is useful to leave this setting turned on so that, subsequently, you have the option of decrypting the contents of any email or files you encrypt.
- **Faster Key Generation**. When this setting is selected, less time is required to generate a new Diffie-Hellman/DSS keypair. This process is speeded up by using a previously calculated set of prime numbers rather than going through the time-consuming process of creating them from scratch each time a new key is generated. However, remember that fast key generation is only implemented for key sizes above 1024 and below 4096. Although it would be unlikely for anyone to crack your key based on their knowledge of these canned prime numbers, some may want to spend the extra time to create a keypair with the maximum level of security.

  The general belief in the cryptographic community is that using canned primes provides no decrease in security for the Diffie-Hellman/DSS algorithms. If this feature makes you uncomfortable, you may turn it off.
- **Show PGPtray icon**. When this check box is selected, you can access many PGP utilities through the convenience of PGPtray.
- **Comment Block**. You can add your comment text in this area. The text you enter here is always included in messages and files that you encrypt or sign. Comments entered in this field appear below the --BEGIN PGP MESSAGE BLOCK-- text header and PGP version number of each message.
- **Cache passphrase while logged on**. Automatically saves your passphrase in memory until you log off your computer. If you select this option, you are prompted for your passphrase once for each initial signing and decrypting task. You will not be prompted to enter it again for the same task until you log off your computer.

Caution: When this setting is selected, it is very important that you log off your computer before leaving it unattended. Your passphrase can remain cached for weeks if you never log off—anyone could read your encrypted messages or encrypt messages with your key while you are away from your computer.

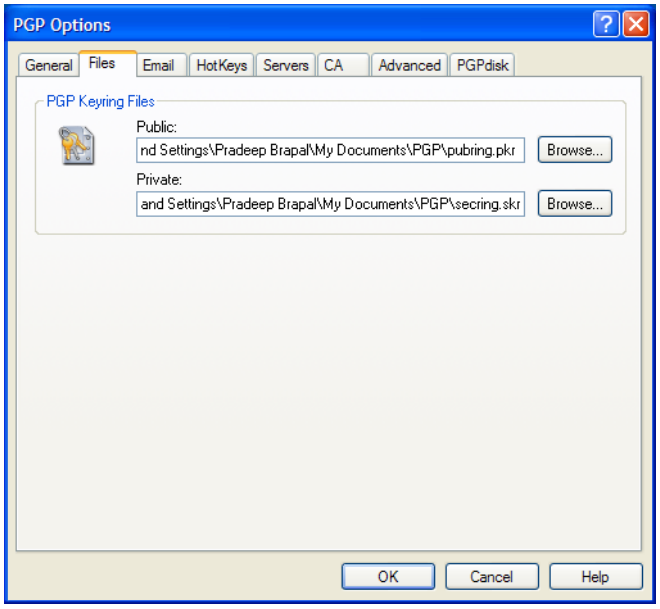
- **Cache passphrase for**. Automatically saves your passphrase in memory for the specified duration of time (in hours: minutes: seconds). If you select this option, you are prompted for your passphrase once for the initial signing or decrypting task. You are not prompted to enter it again until the allotted time you specify has lapsed. The default setting is 2 minutes.

- **Do not cache passphrase**. When this setting is selected, your passphrase is not stored in memory for any amount of time. Therefore, you are required to enter your passphrase for all PGPnet communications, as well as your encrypting, signing, and decrypting tasks.
- **Share passphrase cache among modules**. Automatically saves your passphrase in memory and shares it among other PGP modules. For example, if you enter your passphrase to sign, then you are not prompted for it to decrypt later on. Select this option with the Cache passphrases while logged on option and your passphrase is saved in memory until you log off your computer. Or, select this option with Cache passphrases for and set the duration for which you want to save your passphrase.
- **Number of Passes**. This setting controls how many times the wipe utilities pass over the disk.
- **Warn before user-initiated wiping**. When this setting is selected, a dialog box appears before you wipe a file to give you one last chance to change your mind before PGP securely overwrites the contents of the file and deletes it from your computer.
- **Automatically wipe on delete**. When you delete a file normally by placing it in the Recycle Bin, the name of the file is removed from the file directory, but the data in the file stays on the disk and is still recoverable even after you empty the Recycle Bin. When you enable the Automatically Wipe on Delete option, the Empty Recycle Bin action wipes the contents of the Recycle Bin so that your deleted items can no longer be recovered.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting Files options

Use the Files tab to specify the location of the keyrings used to store your private and public keys.



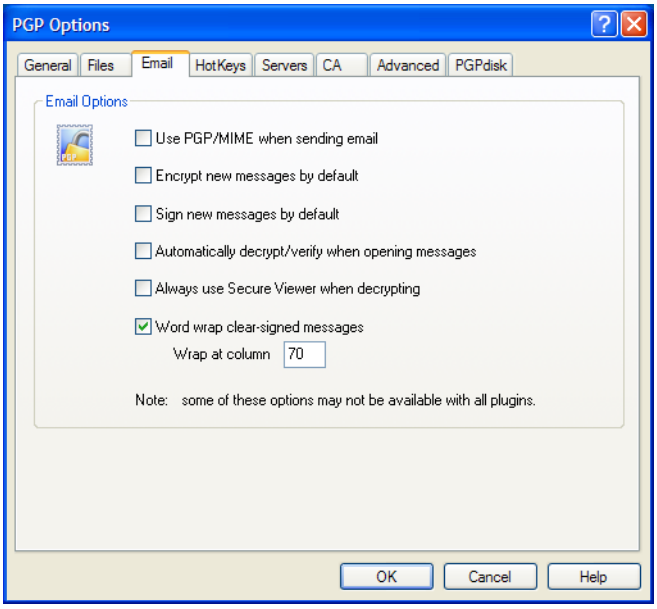
Make your selections for the following options:

- **Public** shows the current location and name of the file where the PGP program expects to find your public keyrings. If you plan to store your public keys in some other location, you must specify this information here. The location you specify can also be used to store all automatic backups of the public keyring.
- **Private** shows the current location and name of the file where the PGP program expects to find your private keyrings. If you plan to store your private keys in some other location, you must specify this information here. Some users like to keep their private keyring on a floppy disk, which they insert like a key whenever they need to sign or decrypt mail. The location you specify can also be used to store all automatic backups of the public keyring.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting Email options

Use the **Email** tab to specify settings for your email application. Not all of the selections apply to every email application.



Make your selections for the following options:

- **Use PGP/MIME when sending mail.** If you are using Eudora and you enable this setting, all of your email messages and file attachments are automatically encrypted to the intended recipient. This setting has no effect on other encryptions you perform from the clipboard, If you enable this setting, all of your email messages and file attachments are automatically encrypted. Some email applications cannot support this feature.
- **Encrypt new messages by default**. If you enable this setting, all of your email messages and file attachments are automatically encrypted. Some email applications cannot support this feature.
- **Sign new messages by default**. If you enable this setting, you are prompted to sign all of your email messages. Some email applications cannot support this feature. This setting has no effect on other signatures you add from the clipboard or with Windows Explorer.
- **Automatically decrypt/verify when opening messages.** If you enable this setting, all of your email messages and file attachments that are encrypted and/or signed are automatically decrypted and verified. Some email applications cannot support this feature.

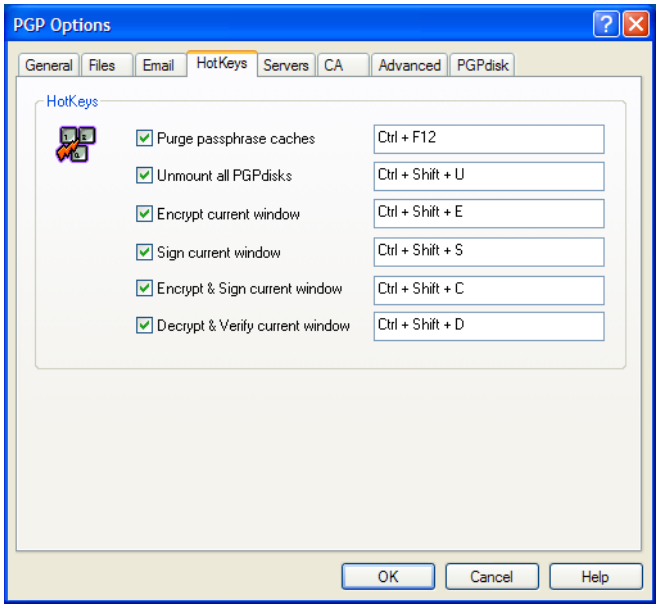
- **Always use Secure Viewer when decrypting.** If you enable this setting, all of your decrypted email messages are displayed in the Secure Viewer window with a special TEMPEST attack prevention font, and they can't be saved in decrypted format. For more information about TEMPEST attacks, see *An Introduction to Cryptography*.
- **Word wrap clear-signed messages at column** [ ]. This setting specifies the column number where a hard carriage return is used to wrap the text in your digital signature to the next line. This feature is necessary because not all applications handle word wrapping in the same way, which could cause the lines in your digitally signed messages to be broken up in a way that cannot be easily read. The default setting is 70, which prevents problems with most applications.

Note: If you change the word-wrap setting in PGP, make sure that it is less than the word-wrap settings in your email application. If you set it to be the same or a greater length, carriage returns may be added that invalidate your PGP signature.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting HotKeys options

Use the HotKeys tab to specify keystroke shortcuts for PGP functions.



Make your selections for the following options:

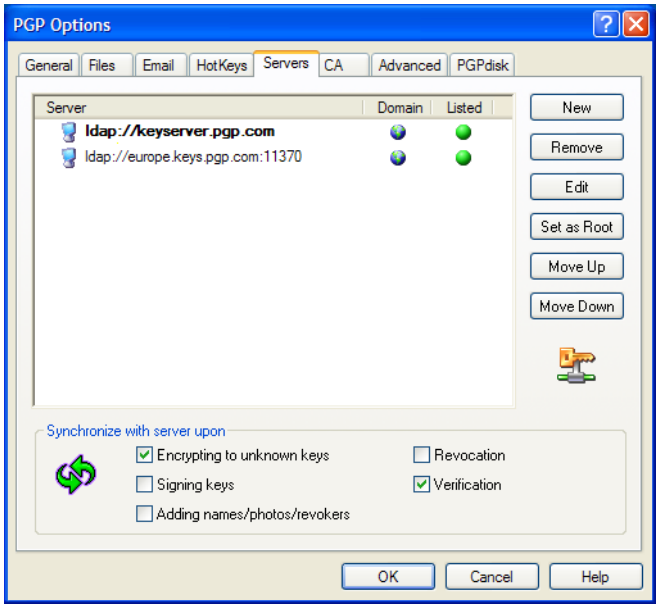
- **Purge passphrase caches**. The default hotkey is Ctrl–F12.
- **Unmount all PGPdisks**. The default hotkey is Ctrl–Shift–U.

- **Encrypt current window.** The default hotkey is Ctrl–Shift–E.
- **Sign current window.** The default hotkey is Ctrl–Shift–S.
- **Encrypt & Sign current window.** The default hotkey is Ctrl–Shift–C.
- **Decrypt & Verify current window.** The default hotkey is Ctrl–Shift–D.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting Servers options

Use the Servers tab to specify settings for the public key servers or directory servers that you are using to send and retrieve public keys, and with which you will automatically synchronize keys.



The box at the top of the screen shows configured servers. How to modify the list of servers and how to add and edit the list of servers is described below.

Make your selections for the following options:

- **Encrypting to unknown keys**. Select this option to have PGP automatically look up unknown recipients on the server to locate users that are not on your keyring when encrypting email.
- **Signing keys**. Select this option to allow keys to which you're adding your signature first to be updated from the server and then your changes sent to the server upon completion of the update.

- **Adding names/photos/revokers**. Select this option to allow keys to which you've added names, photographs, or revokers first to be updated from the server and then your changes sent to the server upon completion of the update. Updating the key beforehand ensures that, for example, the key has not been revoked since you last updated it.
- **Revocation**. Select this option to allow keys you revoke first to be updated from the server and then your changes sent to the server upon completion of the update.
- **Verification**. Select this option to have PGP automatically search and import from the key server when verifying a signed email message or file for which you do not have the sender's public key.

Modifying the list of servers

The buttons on the right side of the list of servers let you modify the list:

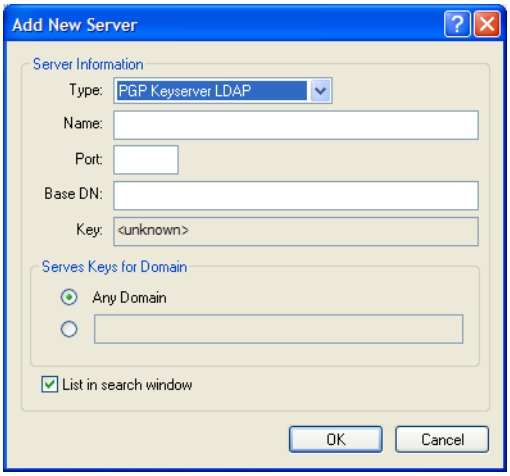
- **New.** Adds a new server to your list (see "Adding and editing servers" on page 145 for more information).
- **Remove**. Removes the currently selected server from your list.
- **Edit**. Allows you to edit server information for the currently selected server.
- **Set As Root**. Identifies the root server that is used for specific corporate operations, such as updating group lists, sending group lists, updating introducers, etc. In corporate settings, your PGP administrator will have already configured this.
- **Move Up** and **Move Down**. Use these buttons to arrange the servers in order of preference.

Adding and editing servers

To add a new server or edit an existing server:

1. Click the **New** button. (If you are editing an existing server, click on the server you want to edit and click **Edit**).

The Add New Server screen appears.



2. In the Type drop-down list, select the type of server to use to access the keyserver. Your choices are:
   - PGP Keyserver HTTP. Select this option if you are using a Web-based PGP Keyserver to store and retrieve PGPkeys.
   - PGP Keyserver LDAP. Select this option if you are using a PGP Keyserver through LDAP to store and retrieve PGPkeys.
   - PGP Keyserver LDAPS. Select this option if you are using a PGP Keyserver through LDAPS to store and retrieve PGPkeys.
   - X.509 Directory LDAP. Select this option if you are using a generic LDAP directory server to store and retrieve X.509 certificates issued by iPlanet CMS or Microsoft Certificate Services.
   - X.509 Directory LDAPS. Select this option if you are using a generic LDAPS directory server to store and retrieve X.509 certificates issued by iPlanet CMS or Microsoft Certificate Services.
3. In the Name box, enter the domain name or IP address of the server. For example, server.pgp.com or 123.45.67.89
4. In the Port box, enter the port number of the server. For example 11371 is used for old-style HTTP key server, 389 is commonly used for LDAP key servers. If you don't know the port number, leave this box blank; the default port number for the type of server you are configuring will be used.
5. The Key box is for LDAPS servers. The server key is used by the server to authenticate the connection. (Key information is not displayed until you connect to the server.)
6. Under Serves Key for Domain, select the **Any Domain** option to allow PGP to send keys from any domain to this keyserver. This setting also applies to automatic searches and updates. It is enabled by default.

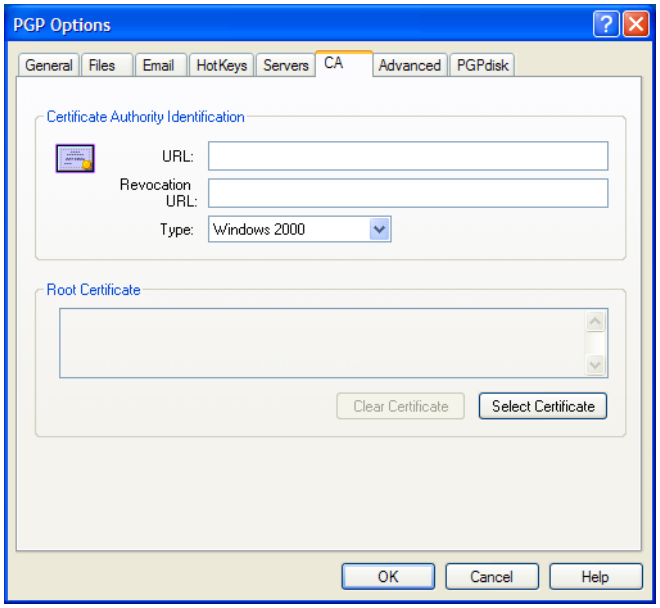
If you want PGP to send only keys from a specific domain to this key server, select the option below **Any Domain**. Then, enter the domain name in the space provided. For example, if you specify the domain pgp.com, only those keys whose email address ends in pgp.com will be sent to this server.

7. Select the **List in search window** check box if you want this key server listed in the PGP Keys Search window.
8. When you have made your selections, click **OK**.

   The Server Information screen disappears and the server you just configured displays in the list.
9. Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting certificate authority (CA) options

Use the CA tab to add your X.509 certificate to your PGP key. Before you can add your X.509 certificate, however, you must first obtain the Root CA certificate from your company's key server.

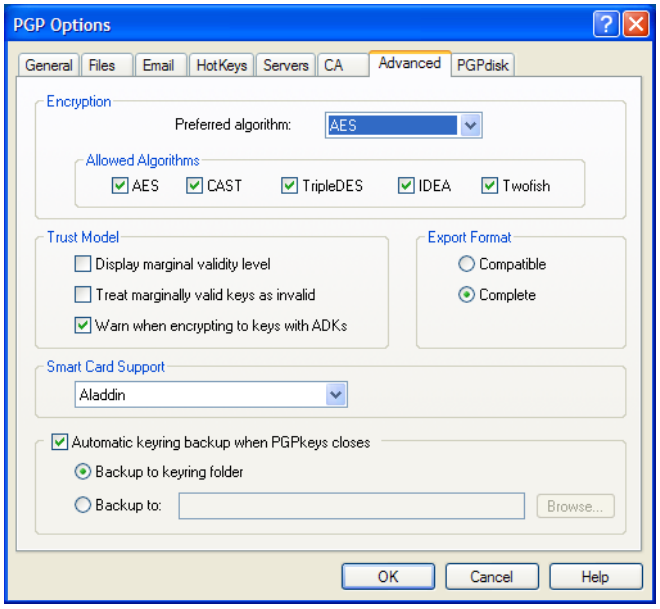


For instructions on how to obtain the Root CA certificate and add an X.509 certificate to your key, see "Adding an X.509 certificate to your PGP key" on page 132.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting Advanced options

Use the Advanced tab to select your preferred encryption algorithm, the allowed algorithms, key trust options, key export format, and automatic keyring backup settings.



Make your selections for the following options:

- **Preferred Algorithm**. Select your preferred algorithm. The choices are:
  - **AES**. The default. The new Advanced Encryption Standard (AES) chosen by the National Institute of Standards and Technology (NIST) is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. It is considered to be both faster and smaller than its competitors. Selecting this option allows PGP to use key and block sizes of 256, 192, and 128 bits (in order of preference).
  - **CAST**. CAST is a 128-bit block cipher. It is a strong, military-grade encryption algorithm, which has a solid reputation for its ability to withstand unauthorized access.
  - **TripleDES**. (If you want to use Triple-DES, then you must make the selection before you generate your keys.) Triple-DES is a U.S. Government algorithm that has withstood the test of time. It's an encryption configuration in which the DES algorithm is used three times with three different keys.
  - **IDEA**. (If you want to use IDEA, then you must make the selection before you generate your keys.) IDEA is the algorithm used for all RSA Legacy keys generated by PGP.

  - **Twofish**. Twofish is a 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES). Rijndael was the chosen algorithm.

  For more information about these algorithms, see An Introduction to Cryptography.

  The Preferred Algorithm choice affects the following:

  - When using conventional encryption, the preferred cipher is used to encrypt.
  - When creating a key, the preferred cipher is recorded as part of the key so that other people will use that algorithm when encrypting to you.

- The **Allowed Algorithms** are recorded as part of the key so that other people will use one of those algorithms when encrypting to you if the preferred algorithm is not available to them.

Caution: Clear the Allowed Algorithms check boxes only if you have suddenly learned that a particular algorithm is insecure. For example, if you become aware that IDEA has been broken, you can deselect that check box and all new keys you generate will have a record that IDEA may not be used when encrypting to you.

  Encrypting to a public key will fail if neither the Preferred Algorithm nor any of the Allowed Algorithms are available to the person encrypting the message.

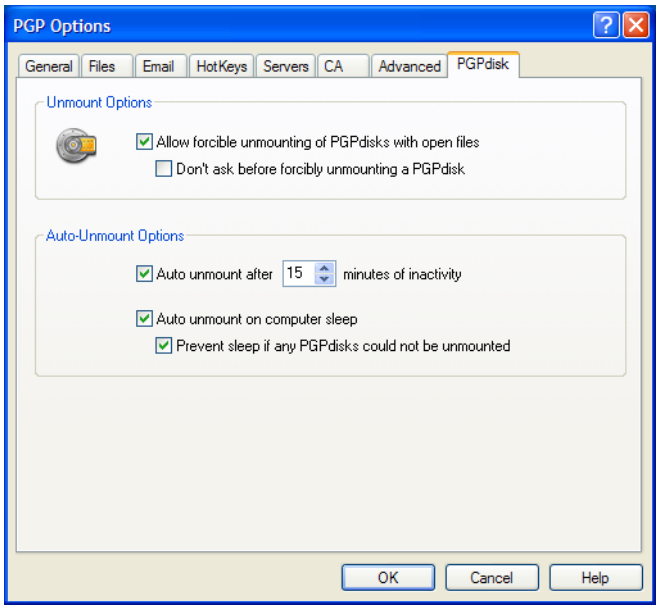
- **Display marginal validity level**. Use this check box to specify whether to display marginally valid keys as such, or simply to show validity as on or off. Marginal validity appears as bar icons having differing shading patterns. On/off validity appears as circle icons; green for valid, gray for invalid (the key has not been validated; it has not been signed by either a trusted introducer or by you)
- **Treat marginally valid keys as invalid**. Use this check box to specify whether to treat all marginally valid keys as invalid. Selecting this option causes the Key Selection dialog box to appear whenever you encrypt to marginally valid keys.
- **Warn when encrypting to keys with ADKs**. Use this check box to specify whether to issue a warning whenever an encrypt-to key has an associated Additional Decryption Key.
- **Export Format**. The options are:
  - **Compatible**: Exports keys in a format compatible with previous versions of PGP.
  - **Complete**: Exports the new key format, which includes photographic IDs and X.509 certificates.

- **Smart card support**. Select the type of smart card you want PGP to support. You can only support one type of smart card at any given time. Your options are:
  - **None.** Select this option if you do not have a smart card reader installed or you do not want PGP to support any type of smart card.
  - **Aladdin.** Select this option if you want to use the Aladdin eToken Pro product line of USB smart cards with PGP.
  - **Gemplus.** Select this option if you want to use GemPlus GemSafe Enterprise brand smart cards with PGP.
  - **Rainbow.** Select this option if you want to use Rainbow iKey 20XX brand smart cards with PGP.
  - **Schlumberger**. Select this option if you want to use Schlumberger Cryptoflex brand smart cards with PGP.
  - **Other**. Select this option if you are using a type of smart card *other* than Aladdin eToken, GemSafe GemPlus, Rainbow, or Schlumberger. You will be asked to enter the filename for the DLL for the card you want PGP to support.
- **Automatic keyring backup when PGPkeys closes**. Select this check box to back up your public and private keyrings automatically when you close PGP.
  - **Back up to keyring folder**. Select this option to store your keyring back up files in the default PGP keyring folder.
  - **Back up to**. Select this option to specify the location in which you want to store your backup files.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

Setting PGP Disk options

The **PGPdisk** tab lets you to specify how you want to unmount existing volumes.



- **Allow forcible unmounting of PGPdisks with open files.** Normally, you can't automatically unmount a PGPdisk volume if any of the files in that volume are open. Checking this option allows forcible unmounting even with open files.

  The **Don't ask before forcibly unmounting a PGPdisk** option allows PGPdisk to automatically unmount a PGPdisk volume without first warning you of any files that may be open.

Caution: You may lose data if you unmount a PGPdisk volume that contains open files. If you select Allow forcible unmounting of PGPdisks with open files you will receive a warning if there are open files in the PGPdisk volume you are unmounting. You are not warned of open files if you select the Don't ask before forcibly unmounting a PGPdisk option.

- **Auto unmount after** [15] **minutes of inactivity.** When checked, this option causes PGPdisk to automatically unmount any mounted PGPdisk volumes when your computer is inactive for the number of minutes in the box. You can set this value from 1 to 999 minutes.

Note: PGPdisk cannot automatically unmount a PGPdisk volume if any of the files in that volume are open.

- **Auto unmount on computer sleep.** When checked, this option causes PGPdisk to automatically unmount any mounted PGPdisk volumes when your computer goes into Sleep mode. (Not all computer models have a sleep mode.)

  Put a checkmark next to **Prevent sleep if any PGPdisk could not be unmounted** if you want to prevent your computer from sleeping if a PGPdisk could not be unmounted.

Click **OK** to save your changes and close the PGP Options screen or select another tab to continue configuring your PGP options.

B Troubleshooting

This appendix presents information about problems you may encounter while using PGP and suggests solutions. The following table lists PGP errors, a possible cause for the error, and a solution.

Error	Cause	Solution
Authentication rejected by remote SKEP connection	The user on the remote side of the network share file connection rejected the key that you provided for authentication.	Use a different key to authenticate the network share file connection, or contact the remote user to assure them that the key you're using is valid.
The PGP memory page locking driver is not functioning correctly.	Could be the result of an incorrect installation, a system failure, or tampering with your system.	Reinstall PGP.
Cannot perform the requested operation because the output buffer is too small.	The output is larger than the internal buffers can handle.	If you are encrypting or signing, you may have to break up the message and encrypt/sign smaller pieces at a time. If you are decrypting or verifying, ask the sender to encrypt/sign smaller pieces and re-send them to you.
Could not encrypt to specified key because it is a sign-only key.	The selected key can only be used for signing.	Choose a different key, or generate a new key that can encrypt data.
Could not sign with specified key because it is an encrypt-only key.	The selected key can only be used for encrypting.	Choose a different key, or generate a new key that can sign data.
Error in domain name system	The destination address you provided is incorrect, or your network connection is misconfigured.	Check to make sure that the destination address you provided is the correct one. If you are sure of this, check your connection to the network.

Error	Cause	Solution
Identical shares cannot be combined	You attempted to combine the same share twice.	If you received the shares from a share file, try choosing a different share file. If you received the shares from the network, you may need to contact the user at the remote location and tell them to send a different set of shares
No secret keys could be found on your keyring.	There are no private keys on your keyring.	Generate your own pair of keys in PGPkeys.
Socket is not connected	The network connection to the PGP key server or to the network share file connection has been broken.	Try re-establishing the connection by repeating the procedure you used to start the connection. If that fails, check your connection to the network.
The action could not be completed due to an invalid file operation.	The program failed to read or write data in a certain file.	The file is probably corrupt. Try altering your PGP Options to use a different file, if possible.
The evaluation time for PGP encrypting and signing has passed. Operation aborted.	The product evaluation time has expired.	Download the freeware version or buy the commercial version of the product.
The keyring contains a bad (corrupted) PGP packet.	The PGP message that you are working with has been corrupted, or your keyring has been corrupted.	Ask the sender to re-send the message if it's a message that you're working with. If it's your keyring, try restoring from your backup keyring.
The keyring file is corrupt.	The program failed to read or write data in a certain file.	There is a file that is probably corrupt or missing. It may or may not be the keyring file. Try using a different file name or path, if possible.
The message/data contains a detached signature.	The signature for the message/file is located in a separate file.	Double-click on the detached signature file first.

Error	Cause	Solution
The passphrase you entered does not match the passphrase on the key.	The passphrase you entered is incorrect.	You may have the CAPS LOCK on, or you simply may have mis-typed the passphrase. Try again.
The PGP library has run out of memory.	The operating system has run out of memory.	Close other running programs. If that doesn't work, you may need more memory in your machine.
The specified user ID was not added because it already exists on the selected key.	You can't add a User ID to a key if there is one just like it already on the key.	Try adding a different user ID, or delete the matching one first.
The specified key could not be found on your keyring.	The key needed to decrypt the current message is not on your keyring.	Ask the sender of the message to re-send the message and make sure they encrypt the message to your public key.
The specified input file does not exist.	The file name typed in does not exist.	Browse to find the exact name and path of the file you want.
There is not enough random data currently available.	The random number generator needs more input in order to generate good random numbers.	When prompted, move the mouse around, or press random keys, in order to generate input.
There was an error during the writing of the keyring or the exported file.	The program failed to write data to a certain file.	Your hard drive may be full, or if the file is on a floppy, the floppy is not present in the floppy drive.
There was an error opening or writing the keyring or the output file.	A file that was needed couldn't be opened.	Make sure the settings in your PGP Options is correct. If you've recently deleted files in the directory that you installed PGP, you may need to re-install the product.
This key is already signed by the specified signing key.	You can't sign a key that you have already signed.	You may have accidentally picked the wrong key. If so, choose a different key to sign.

Error	Cause	Solution
Unable to perform operation because this file is read-only or otherwise protected. If you store your keyring files on removable media the media may not be inserted.	A file that was needed is set to read-only or is being used by another program.	Close other programs that may be accessing the same files as the program you are running. If you keep your keyring files on a floppy disk, make sure that the floppy disk is in the floppy drive.

C Biometric Word Lists

By Philip Zimmermann and Patrick Juola

PGP uses a special list of words to convey binary information in an authenticated manner over a voice channel, such as a telephone, via biometric signatures. The human voice that speaks the words, if recognized by the listener, serves as a means of biometric authentication of the data carried by the words. The word list serves the same purpose as the military alphabet, which is used to transmit letters over a noisy radio voice channel. But the military alphabet has 26 words, each word representing one letter. For our purposes, our list has 256 carefully selected phonetically distinct words to represent the 256 possible byte values of 0 to 255.

We created a word list for reading binary information over the phone, with each word representing a different byte value. We tried to design the word list to be useful for a variety of applications. The first application we had envisioned was to read PGP public key fingerprints over the phone to authenticate the public key. In that case, the fingerprint is 20 bytes long, requiring 20 words to be read aloud. Experience has shown it to be fairly tedious and error prone to read that many bytes in hexadecimal, so it seems worth using a word list to represent each byte by a word.

Some applications may require transmitting even lengthier byte sequences over the phone, for example, entire keys or signatures. This may entail reading more than a hundred bytes. Using words instead of hex bytes seems even more justified in that case.

When reading long sequences of bytes aloud, errors may creep in. The kinds of error syndromes you get on human-spoken data are different than they are for transmitting data through a modem. Modem errors usually involve flipped bits from line noise. Error detection methods for modems usually involve CRCs to be added, which are optimized for detecting line noise bursts. However, random sequences of spoken human words usually involves one of three kinds of errors: 1) transposition of two consecutive words, 2) duplicate words, or 3) omitted words. If we are to design an error detection scheme for this kind of data transmission channel, we should make one that is optimized for these three kinds of errors. Zhahai Stewart suggested a good scheme (in personal conversation with me in 1991) for error detection of these errors.

Stewart's scheme for error detection while reading aloud long sequences of bytes via a word list entails using not one, but two lists of words. Each list contains 256 phonetically distinct words, each word representing a different byte value between 0 and 255. The two lists are used alternately for the even-offset bytes and the odd-offset bytes in the byte sequence.

For example, the first byte (offset 0 in the sequence) is used to select a word from the even list. The byte at offset 1 is used to select a byte from the odd list. The byte at offset 2 selects a word from the even list again, and the byte at offset 3 selects from the

odd list again. Each byte value is actually represented by two different words, depending on whether that byte appears at an even or an odd offset from the beginning of the byte sequence. For example, suppose the word "adult" and the word "amulet" each appears in the same corresponding position in the two word lists, position 5. That means that the repeating three-byte sequence 05 05 05 is represented by the 3-word sequence "adult, amulet, adult."

This approach makes it easy to detect all three kinds of common errors in spoken data streams: transposition, duplication, and omission. A transposition will result in two consecutive words from the even list followed by two consecutive words from the odd list (or the other way around). A duplication will be detected by two consecutive duplicate words, a condition that cannot occur in a normal sequence. An omission will be detected by two consecutive words drawn from the same list.

To facilitate the immediate and obvious detection by a human of any of the three error syndromes described above, without computer assistance, we made the two lists have one obviously different property: The even list contains only two-syllable words, while the odd list contains only three-syllable words. That suggestion came from Patrick Juola, a computational linguist.

PGPfone was the application that precipitated the actual development of the word list by Juola and Zimmermann. PGPfone is an application that turns your computer into a secure telephone. We used it to authenticate PGPfone's initial Diffie-Hellman key exchange without using digital signatures and public key infrastructures. We knew we would end up using it for authenticating PGP key fingerprints when we applied it to PGP later.

The idea behind building the word lists was to develop a metric to measure the phonetic distance between two words, then use that as a goodness measure to develop a full list. Grady Ward provided us with a large collection of words and their pronunciations, and Patrick Juola used genetic algorithms to evolve the best subset of Ward's list.

To briefly summarize what he did, he made a large population of guesses and let the population "sexually reproduce" by exchanging words with other guesses—and, like biological evolution, the better guesses survived into the next generation. After about 200 generations, the list had mostly stabilized into a best guess, with far greater phonetic distance between the words than what we started with in the initial guess lists.

The first major hurdle was the development of the metric. Linguists have studied sound production and perception for decades, and there is a standard feature set used to describe sounds in English. For example, say the words "pun," "fun," "dun," and "gun" (go ahead, try it), and notice how your tongue keeps moving back in your mouth on each word. Linguists call this the "place of articulation," and noises that are very different in this feature sound different to English speakers. Combining the features of all the sounds in a word gives us a representation of the sound of the entire word—and we can compute the phonetic distance between a pair of words.

Actually, it wasn't that simple. We didn't know how to weight the various features, certain word-level features like accents were hard to represent, and the feature-based analysis simply fails for certain sounds. There were also a few other more subtle criteria; for example, we wanted the words to be common enough to be universally recognizable, but not so common as to be boring—and we didn't want confusing words like "repeat" or "begin" or "error". Some sound features are less perceptible to non-native-English speakers; for example, some Japanese speakers might hear and pronounce "r" and "l" the same way. It would be nice if the words were short enough that you could fit enough of them on a small LCD display. Large consonant clusters ("corkscrew" has five pronounced consonants in a row) are sometimes hard to say, especially to non-English speakers. One way or another, we tried to incorporate all these criteria into a filter on the initial dictionary list or into the distance metric itself.

After the computer evolved the winning list, we looked at it. Yes, the words were phonetically distinct. But many of them looked like a computer picked them, not a human. A lot of them were just ugly and dumb. Some were repugnant, and some were bland and wimpy. So we applied some "wetware" augmentation to the list. Some words were deleted, and replaced by some human-chosen words. We had the computer check the new words against the list to see if they were phonetically distant from the rest of the list. We also tried to make the words not come too close to colliding phonetically with the other words in the larger dictionary, just so that they would not be mistaken for other words not on the list.

There were a variety of selection criteria that Juola used in his algorithms. He published a paper on it that goes into more detail. This document is just a brief overview of how we built the list.

I'm not entirely happy with the word list. I wish it had more cool words in it, and less bland words. I like words like "Aztec" and "Capricorn", and the words in the standard military alphabet. While we'd like to reserve the right to revise the list at some future time, it's not likely, due to the legacy problems that this initial version will create. This version of the list was last modified in September 1998.

Two Syllable Word List

aardvark	absurd	accrue	acme	adrift
adult	afflict	ahead	aimless	Algol
allow	alone	ammo	ancient	apple
artist	assume	Athens	atlas	Aztec
baboon	backfield	backward	banjo	beaming
bedlamp	beehive	beeswax	befriend	Belfast
berserk	billiard	bison	blackjack	blockade
blowtorch	bluebird	bombast	bookshelf	brackish
breadline	breakup	brickyard	briefcase	Burbank
button	buzzard	cement	chairlift	chatter
checkup	chisel	choking	chopper	Christmas
clamshell	classic	classroom	cleanup	clockwork
cobra	commence	concert	cowbell	crackdown
cranky	crowfoot	crucial	crumpled	crusade
cubic	dashboard	deadbolt	deckhand	dogsled
dragnet	drainage	dreadful	drifter	dropper
drumbeat	drunken	Dupont	dwelling	eating
edict	egghead	eightball	endorse	endow
enlist	erase	escape	exceed	eyeglass
eyetooth	facial	fallout	flagpole	flatfoot
flytrap	fracture	framework	freedom	frighten
gazelle	Geiger	glitter	glucose	goggles
goldfish	gremlin	guidance	hamlet	highchair
hockey	indoors	indulge	inverse	involve
island	jawbone	keyboard	kickoff	kiwi
klaxon	locale	lockup	merit	minnow
miser	Mohawk	mural	music	necklace
Neptune	newborn	nightbird	Oakland	obtuse
offload	optic	orca	payday	peachy
pheasant	physique	playhouse	Pluto	preclude
prefer	preshrunk	printer	prowler	pupil
puppy	python	quadrant	quiver	quota
ragtime	ratchet	rebirth	reform	regain
reindeer	rematch	repay	retouch	revenge
reward	rhythm	ribcage	ringbolt	robust
rocker	ruffled	sailboat	sawdust	scallion
scenic	scorecard	Scotland	seabird	select
sentence	shadow	shamrock	showgirl	skullcap
skydive	slingshot	slowdown	snapline	snapshot
snowcap	snowslide	solo	southward	soybean
spaniel	spearhead	spellbind	spheroid	spigot
spindle	spyglass	stagehand	stagnate	stairway
standard	stapler	steamship	sterling	stockman
stopwatch	stormy	sugar	surmount	suspense
sweatband	swelter	tactics	talon	tapeworm
tempest	tiger	tissue	tonic	topmost
tracker	transit	trauma	treadmill	Trojan
trouble	tumor	tunnel	tycoon	uncut
unearth	unwind	uproot	upset	upshot
vapor	village	virus	Vulcan	waffle
wallet	watchword	wayside	willow	woodlark
Zulu				

Three Syllable Word List

adroitness	adviser	aftermath	aggregate	alkali
almighty	amulet	amusement	antenna	applicant
Apollo	armistice	article	asteroid	Atlantic
atmosphere	autopsy	Babylon	backwater	barbecue
belowground	bifocals	bodyguard	bookseller	borderline
bottomless	Bradbury	bravado	Brazilian	breakaway
Burlington	businessman	butterfat	Camelot	candidate
cannonball	Capricorn	caravan	caretaker	celebrate
cellulose	certify	chambermaid	Cherokee	Chicago
clergyman	coherence	combustion	commando	company
component	concurrent	confidence	conformist	congregate
consensus	consulting	corporate	corrosion	councilman
crossover	crucifix	cumbersome	customer	Dakota
decadence	December	decimal	designing	detector
detergent	determine	dictator	dinosaur	direction
disable	disbelief	disruptive	distortion	document
embezzle	enchanting	enrollment	enterprise	equation
equipment	escapade	Eskimo	everyday	examine
existence	exodus	fascinate	filament	finicky
forever	fortitude	frequency	gadgetry	Galveston
getaway	glossary	gossamer	graduate	gravity
guitarist	hamburger	Hamilton	handiwork	hazardous
headwaters	hemisphere	hesitate	hideaway	holiness
hurricane	hydraulic	impartial	impetus	inception
indigo	inertia	infancy	inferno	informant
insincere	insurgent	integrate	intention	inventive
Istanbul	Jamaica	Jupiter	leprosy	letterhead
liberty	maritime	matchmaker	maverick	Medusa
megaton	microscope	microwave	midsummer	millionaire
miracle	misnomer	molasses	molecule	Montana
monument	mosquito	narrative	nebula	newsletter
Norwegian	October	Ohio	onlooker	opulent
Orlando	outfielder	Pacific	pandemic	Pandora
paperweight	paragon	paragraph	paramount	passenger
pedigree	Pegasus	penetrate	perceptive	performance
pharmacy	phonetic	photograph	pioneer	pocketful
politeness	positive	potato	processor	provincial
proximate	puberty	publisher	pyramid	quantity
racketeer	rebellion	recipe	recover	repellent
replica	reproduce	resistor	responsive	retraction
retrieval	retrospect	revenue	revival	revolver
sandalwood	sardonic	Saturday	savagery	scavenger
sensation	sociable	souvenir	specialist	speculate
stethoscope	stupendous	supportive	surrender	suspicious
sympathy	tambourine	telephone	therapist	tobacco
tolerance	tomorrow	torpedo	tradition	travesty
trombonist	truncated	typewriter	ultimate	undaunted
underfoot	unicorn	unify	universe	unravel
upcoming	vacancy	vagabond	vertigo	Virginia
visitor	vocalist	voyager	warranty	Waterloo
whimsical	Wichita	Wilmington	Wyoming	yesteryear
Yucatan				

Glossary

AES (Advanced Encryption Standard)
NIST approved encryption standards, usually used for the next 20 - 30 years. Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen, was chosen as the new AES in October 2000.

Algorithm (encryption)
A set of mathematical rules (logic) used in the processes of encryption and decryption.

Algorithm (hash)
A set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

Anonymity
Of unknown or undeclared origin or authorship, concealing an entity's identification.

ANSI (American National Standards Institute)
Develops standards through various Accredited Standards Committees (ASC). The X9 committee focuses on security standards for the financial services industry.

ASCII-armored text
Binary information that has been encoded using a standard, printable, 7-bit ASCII character set, for convenience in transporting the information through communication systems. In the PGP program, ASCII armored text files are given the default filename extension, and they are encoded and decoded in the ASCII radix-64 format.

Asymmetric keys
A separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information can not be used to decrypt the same data.

Authentication
The determination of the origin of encrypted information through the verification of someone's digital signature or someone's public key by checking its unique fingerprint.

Authorization certificate
An electronic document to prove one's access or privilege rights, also to prove one is who they say they are.

Authorization
To convey official sanction, access or legal power to an entity.

Backdoor
A cipher design fault, planned or accidental, which allows the apparent strength of the design to be easily avoided by those who know the trick. When the design background of a cipher is kept secret, a back door is often suspected.

Blind signature
Ability to sign documents without knowledge of content, similar to a notary public.

Block cipher
A symmetric cipher operating on blocks of plain text and cipher text, usually 64 bits.

CA (Certificate Authority)
A trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to their public key.

CAPI (Crypto API)
Microsoft's crypto API for Windows-based operating systems and applications.

CAST
A 64-bit block cipher using 64-bit key, six S-boxes with 8-bit input and 32-bit output, developed in Canada by Carlisle Adams and Stafford Tavares.

Certificate (digital certificate)
An electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

Certification
Endorsement of information by a trusted entity.

Certify
To sign another person's public key.

Certifying authority
One or more trusted individuals who are assigned the responsibility of certifying the origin of keys and adding them to a common database.

Ciphertext
Plaintext converted into a secretive format through the use of an encryption algorithm. An encryption key can unlock the original plaintext from ciphertext.

Clear-signed message
Messages that are digitally signed but not encrypted.

Clear text
Characters in a human readable form or bits in a machine-readable form (also called *plain text*).

Compression function
A compression function takes a fixed-sized input and returns a shorter, fixed sized output.

Corporate signing key
A public key that is designated by the security officer of a corporation as the system-wide key that all corporate users trust to sign other keys.

Conventional encryption
Encryption that relies on a common passphrase instead of public key cryptography. The file is encrypted using a session key, which encrypts using a passphrase that you will be asked to choose.

Cryptanalysis
The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

CRYPTOKI
Same as PKCS #11.

Cryptography
The art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.

Cryptosystem
A system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.

Data integrity
A method of ensuring information has not been altered by unauthorized or unknown means.

Decryption
A method of unscrambling encrypted information so that it becomes legible again. The recipient's private key is used for decryption.

denial of service attack
An assault, usually planned, that seeks to disrupt Web access. A denial of service attack overwhelms an Internet server with connection requests that cannot be completed. In so doing, it causes the server to become so busy attempting to respond to the attack that it ignores legitimate requests for connections.

DES (Data Encryption Standard)
A 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over 20 years, adopted in 1976 as FIPS 46.

Dictionary attack
A calculated brute force attack to reveal a password by trying obvious and logical combinations of words.

Diffie-Hellman
The first public key algorithm, invented in 1976, using discrete logarithms in a finite field.

Digital cash
Electronic money that is stored and transferred through a variety of complex protocols.

Direct trust
An establishment of peer-to-peer confidence.

Digital signature
See signature.

DSA (Digital Signature Algorithm)
A public key digital signature algorithm proposed by NIST for use in DSS.

DSS (Digital Signature Standard)
A NIST proposed standard (FIPS) for digital signatures using DSA.

ECC (Elliptic Curve Cryptosystem)
A unique method for creating public key algorithms based on mathematical curves over finite fields or with large prime numbers.

EES (Escrowed Encryption Standard)
A proposed U.S. government standard for escrowing private keys.

Elgamal scheme
Used for both digital signatures and encryption based on discrete logarithms in a finite field; can be used with the DSA function.

Encryption
A method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.

Fingerprint
A uniquely identifying string of numbers and characters used to authenticate public keys. This is the primary means for checking the authenticity of a key. See *Key Fingerprint*.

FIPS (Federal Information Processing Standard)
A U.S. government standard published by NIST.

Firewall
A combination of hardware and software that protects the perimeter of the public/private network against certain attacks to ensure some degree of security.

Hash function
A one way function that takes an input message of arbitrary length and produces a fixed length digest.

Hierarchical trust
A graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 issuing certifying authorities.

HTTP (HyperText Transfer Protocol)
A common protocol used to transfer documents between servers or from a server to a client.

Hexadecimal
Hexadecimal describes a base-16 number system. That is, it describes a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. (Note that we're using "16" here as a decimal number to explain a number that would be "10" in hexadecimal.) The hexadecimal numbers are 0-9 and then use the letters A-F.

IDEA (International Data Encryption Standard)
A 64-bit block symmetric cipher using 128-bit keys based on mixing operations from different algebraic groups. Considered one of the strongest algorithms.

Implicit trust
Implicit trust is reserved for keypair*s* located on your local keyring. If the private portion of a keypair is found on your keyring, PGP assumes that you are the owner of the keypair and that you implicitly trust yourself.

Integrity
Assurance that data is not modified (by unauthorized persons) during storage or transmittal.

Introducer
A person or organization who is allowed to vouch for the authenticity of someone's public key. You designate an introducer by signing their public key.

ISO (International Organization for Standardization)
Responsible for a wide range of standards, like the OSI model and international relationship with ANSI on X.509.

Key
A digital code used to encrypt and sign and decrypt and verify messages and files. Keys come in keypairs and are stored on keyrings.

Key escrow/recovery
A practice where a user of a public key encryption system surrenders their private key to a third party thus permitting them to monitor encrypted communications.

Key exchange
A scheme for two or more nodes to transfer a secret session key across an unsecured channel.

Key fingerprint
A uniquely identifying string of numbers and characters used to authenticate public keys. For example, you can telephone the owner of a public key and have him or her read the fingerprint associated with their key so you can compare it with the fingerprint on your copy of their public key to see if they match. If the fingerprint does not match, then you know you have a bogus key.

Key ID
A legible code that uniquely identifies a keypair. Two keypairs may have the same user ID, but they will have different Key IDs.

Key length
The number of bits representing the key size; the longer the key, the stronger it is.

Key management
The process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.

keypair
A public key and its complimentary private key. In public-key cryptosystems, like the PGP program, each user has at least one keypair.

Keyring
A set of keys. Each user has two types of keyrings: a private keyring and a public keyring.

Key splitting or "secret sharing"
The process of dividing up a private key into multiple pieces, and share those pieces among a group of people. A designated number of those people must bring their shares of the key together to use the key.

LDAP (Lightweight Directory Access Protocol)
A simple protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet.

Message digest
A compact "distillate" of your message or file checksum. It represents your message, such that if the message were altered in any way, a different message digest would be computed from it.

Meta-introducer
A trusted introducer of trusted introducers.

MIC (Message Integrity Check)
Originally defined in PEM for authentication using MD2 or MD5. Micalg (message integrity calculation) is used in secure MIME implementations.

MIME (Multipurpose Internet Mail Extensions)
A freely available set of specifications that offers a way to interchange text in languages with different character sets, and multimedia email among many different computer systems that use Internet mail standards.

Non-repudiation
Preventing the denial of previous commitments or actions.

One-way hash
A function of a variable string to create a fixed length value representing the original pre-image, also called message digest, fingerprint, message integrity check (MIC).

Passphrase
An easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

Password
A sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

PGP/MIME
An IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847, currently deployed in PGP 5.0 and later versions.

PKCS (Public Key Crypto Standards)
A set of *de facto* standards for public key cryptography developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, RSA, and Sun) that includes algorithm-specific and algorithm-independent implementation standards. Specifications defining message syntax and other protocols controlled by RSA Data Security, Inc.

PKI (Public Key Infrastructure)
A widely available and accessible certificate system for obtaining an entity's public key with some degree of certainty that you have the "right" key and that it has not been revoked.

Plaintext
Normal, legible, un-encrypted, unsigned text.

Private key
The secret portion of a keypair-used to sign and decrypt information. A user's private key should be kept secret, known only to the user.

Private keyring
A set of one or more private keys, all of which belong to the owner of the private keyring.

Public key
One of two keys in a keypair-used to encrypt information and verify signatures. A user's public key can be widely disseminated to colleagues or strangers. Knowing a person's public key does not help anyone discover the corresponding private key.

Public keyring
A set of public keys. Your public keyring includes your own public key(s).

Public-key cryptography
Cryptography in which a public and private keypair is used, and no security is needed in the channel itself.

Random number
An important aspect to many cryptosystems, and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources, and usually involve the use of special hardware.

Revocation
Retraction of certification or authorization.

RFC (Request for Comment)
An IETF document, either FYI (For Your Information) RFC sub-series that are overviews and introductory or STD RFC sub-series that identify specify Internet standards. Each RFC has an RFC number by which it is indexed and by which it can be retrieved (www.ietf.org).

Rijndael
A block cipher designed by Joan Daemen and Vincent Rijmen, chosen as the new Advanced Encryption Standard (AES). It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit in size and either can be increased by increments of 32 bits.

RSA
Short for RSA Data Security, Inc.; or referring to the principals - Ron Rivest, Adi Shamir, and Len Adleman; or referring to the algorithm they invented. The RSA algorithm is used in public key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.

secret sharing
See Key Splitting.

secure channel
A means of conveying information from one entity to another such that an adversary does not have the ability to reorder, delete, insert, or read (SSL, IPSec, whispering in someone's ear).

self-signed key
A public key that has been signed by the corresponding private key for proof of ownership.

session key
The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

sign
To apply a signature.

signature
A digital code created with a private key. Signatures allow authentication of information by the process of signature verification. When you sign a message or file, the PGP program uses your private key to create a digital code that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature.

S/MIME (Secure Multipurpose Mail Extension)
A proposed standard developed by Deming software and RSA Data Security for encrypting and/or authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1), and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet.

SSL (Secure Socket Layer)
Developed by Netscape to provide security and privacy over the Internet. Supports server and client authentication and maintains the security and integrity of the transmission channel. Operates at the transport layer and mimics the "sockets library," allowing it to be application independent. Encrypts the entire communication channel and does not support digital signatures at the message level.

symmetric algorithm
Also known as conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist: Block and Stream.

subkey
A subkey is a Diffie-Hellman encryption key that is added as a subset to your master key. Once a subkey is created, you can expire or revoke it without affecting your master key or the signatures collected on it.

Text
Standard, printable, 7-bit ASCII text.

Timestamping
Recording the time of creation or existence of information.

TLS (Transport Layer Security)
An IETF draft, version 1 is based on the Secure Sockets Layer (SSL) version 3.0 protocol, and provides communications privacy over the Internet.

TLSP (Transport Layer Security Protocol)
ISO 10736, draft international standard.

Triple DES
An encryption configuration in which the DES algorithm is used three times with three different keys.

Trusted
A public key is said to be trusted by you if it has been validated by you or by someone you have designated as an introducer.

Trusted introducer
Someone whom you trust to provide you with keys that are valid. When a trusted introducer signs another person's key, you trust that the person's key is valid, and you do not need to verify the key before using it.

Twofish
A new 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).

User ID
A text phrase that identifies a keypair. For example, one common format for a user ID is the owner's name and email address. The user ID helps users (both the owner and colleagues) identify the owner of the keypair.

Validity
Indicates the level of confidence that the key actually belongs to the alleged owner.

Verification
The act of comparing a signature created with a private key to its public key. Verification proves that the information was actually sent by the signer, and that the message has not been subsequently altered by anyone else.

Web of trust
A distributed trust model used by PGP to validate the ownership of a public key where the level of trust is cumulative, based on the individuals' knowledge of the introducers.

X.509
An ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature, as well as other possible extensions.

Index

A

about
- PGP keyrings 113
- PGP Wipe utility 39, 45
- PGPdisk volumes 91

accessing
- PGPdisk 73

adding
- a photo ID to a key 125
- a Root CA certificate to your key 132
- combining groups 33

alternate passphrases
- adding to PGPdisk 83

attributes
- changing your keyrings' 114–118
- viewing your keyrings' 114–118

Auto unmount preference
- after x minutes of inactivity 85
- on computer sleep 159

automatic
- mounting of PGPdisk volumes 77, 86
- unmounting of PGPdisk volumes 85, 159

C

Certificate server. See key server

changing
- a passphrase for a PGPdisk volume 82
- your passphrase 124

checking
- authenticity of a key 112

conventional encryption 29, 31, 38, 62

creating
- a custom key pair 99
- a key pair on a smart card 66
- a new PGPdisk volume 75
- recipient groups 32

custom key
- creating 99

D

decrypting
- email 34
- ICQ messages 55
- using PGPtray 38
- with split keys 39

default key pair
- specifying 118

deleting
- a subkey 129
- digital signatures 119
- files 39, 45
- keys
  - from a smart card 70
  - from your keyring 119
- recipient groups 33
- user IDs 119
- using Secure Wipe 39, 45

designated revoker
- properties 129

Diffie-Hellman/DSS keys
- an overview of 95

digital signature
- deleting 119

disks
- deleting free space 39, 45
- scheduled wiping 41, 49
- wiping files from 39, 45

distributing
- PGPdisk volumes 87

distribution lists
- adding members to a group list 33
- combining groups 33
- creating a group 32
- deleting a group 33
- deleting a member 33

E

email
combining recipient groups 33
copying public keys from 111
creating recipient groups 32
decrypting 34, 35
deleting recipient groups 33
encrypting 27, 34
to groups of people 32
including your public key in 109
receiving private 27
sending private 27
signing 27, 34
verifying 34, 35
encrypting
email 27, 34, 35
to groups of people 32
ICQ messages 59
encryption options
email
conventional 29, 31, 62
Secure Viewer 28, 30
files
conventional 38
Secure Viewer 38
self decrypting archive 38
text output 38
wipe original 38
Entrust 133
Eudora 34
with PGP/MIME 34
without PGP/MIME 35
examining
key properties 120
smart card properties 68
exchanging
PGPdisk volumes 87
public keys
obtaining others' 110–112
via ICQ 56
exporting
keys, to files 109
your key from a smart card 69

F

files
deleting 39, 45
exporting public keys to 109
importing public keys from 112
wiping 39, 45
fingerprints
example of hexadecimal view 121
example of word list view 121
folder wiping
scheduling 41, 49
forgotten passphrase 104
Free Space Wipe 39, 45
scheduling tasks 41, 49

G

generating
a custom key pair 99
a key pair on a smart card 66
granting
trust for key validations 123
groups
adding members 33
combining groups 33
creating 32
deleting 33

H

HTTP (HyperText Transfer Protocol)
definition 175

I

ICQ
decrypting messages 55
encrypting messages 59
exchanging keys 56
using the PGP ICQ Wizard 57
importing
Pkcs-12 X.509 private keys 112
private keys 112
public keys, from files 112
iPlanet CMS 133

K

key ID
properties 127
key pair
copying to a smart card 71
examining 99
specifying default 118
key reconstruction server
restore your key from 143
send your key to 105
key server
getting someone's public key from 110
searching 110
sending your public key to 108
updating your key on the server 141
using to circulate revoke keys 131
key size
Diffie-Hellman portion 100
DSS portion 100
setting 100, 128
trade-offs 100, 128
keyrings
changing attributes of 114–118
description of 113
location of 113
storing elsewhere 113
viewing attributes of 114–118
keys
adding a photo ID 125
adding your Microsoft Exchange Server ID to 102
copying a key pair to a smart card 71
creating on a smart card 66
deleting from your keyring 119
examining 99
exporting from a smart card 69
granting trust for validations 123
lost 104, 143
managing 113
on a smart card 68
reappearing on server 143
reconstructing 104, 143
rejoining a split key 138
removing signatures 142
removing user names 142
replacing a photo ID 126
revoking 131
setting size of 100, 128
signing 122
updating on a key server 141
verifying authenticity of 112

L

legitimacy
determining a key's 112
Lotus Notes
decrypting and verifying with 63
encrypting with 61
signing with 61

M

managing
keys 113
Microsoft Exchange Server user ID
adding to your new key 102
MIME standard
using to decrypt email 34, 35
mounting PGPdisk volumes 78
automatically 77, 86
on a remote server 86

N

Net Tools PKI 133
Novell GroupWise 36

O

obtaining
  others' public keys 110–112
options
  Email 149
  PGPdisk 158
overview
  of Diffie-Hellman keys 95
  of PGPdisk volumes 91
  of RSA keys 95
  of RSA Legacy keys 95

P

passphrase
  adding alternate ones for PGPdisk 83
  as a protection method for PGPdisk 77
  changing 124
  changing on smart card 72
  changing yours for PGPdisk 82
  forgotten 104, 143
  setting 24, 98, 101, 144
  suggestions for 144
PGP
  troubleshooting 161
PGP Free Space Wiper
  using 39, 45
PGP/MIME standard
  overview 36
  using to decrypt email 34, 35
PGPdisk
  CAST encryption algorithm 91
  changing your passphrase 82
  creating a new volume 75
  encryption algorithms 91
  security precautions 92
    memory static ion migration 92
    passphrase erasure 92
    tips for the user 93
    virtual memory protection 92
  setting unmount preferences 85
  Twofish encryption algorithm 92
PGPdisk preferences
  automatic unmounting 159
PGPdisk volumes
  backing up 86
  changing the size of 88
  exchanging 87
  mounting 78
  nesting 91
  overview 91
  unmounting 78, 79
  unmounting automatically 85, 159
PGPkeys window
  Creation label 118
  examining keys' properties 120
    Key ID 127
  Size label 117
  Trust label 118
  uses 114
  Validity label 117
PGPtray
  using 38
photo ID
  adding to a key 125
  removing from a key 126
Pkcs-12 keys
  obtaining 112
private keys
  importing Pkcs-12 X.509 112
  location of 113

public keys
add or remove for a PGPdisk file 78
advantages of sending to key server 108
copying from a smart card 69
copying from email messages 111
exporting to files 109
getting from a key server 110
importing from files 112
including in an email message 109
location of 113
obtaining others' 110–112
searching key server 110
sending to key server 108
signing 122

R

receiving
private email 27
recipient groups
combining groups 33
creating 32
deleting 33
deleting a group 33
recipients
groups of 32
reconstructing your key 104, 143
rejoining a split key 138
removing
a photo ID from a key 126
a subkey 129
files, using Secure Wipe 39, 45
keys from a smart card 70
revoker
viewing key properties 129
revoking
a subkey 128
keys 131
Root CA certificates 132
RSA keys
an overview of 95
RSA Legacy keys
an overview of 95

S

scheduling
folder wiping 41, 49
free space wiping 41, 49
the Free Space Wiper 41, 49
searching key server 110
Secure Viewer
email encryption option 27
with previous versions 28, 30
Secure Wipe
using 39, 45
Self Decrypting Archive (SDA)
creating 38
sending
private email 27
servers
mounting PGPdisk volumes on 86
servers. See also key servers
setting
passphrase for a key 24, 98, 101, 144
signing 119
email 27, 34
keys 122
public keys 122
with split keys 39
sleep mode
unmounting PGPdisk in 159
smart card
changing passphrase 72
copying a key pair to 71
copying your public key from 69
creating a new key pair on 66
viewing properties of 68
wiping 70
starting
PGPdisk 73

subkey
creating new 127
expiration 127
properties 127
removing 129
revoking 128
size 127
validity 127

T

tasks
scheduled freespace wiping 41, 49
TEMPEST attacks
see also Secure Viewer
text output 38
troubleshooting
PGP 161
trust
granting for key validations 123

U

unmounting
PGPdisk volumes 78, 79
Auto unmount 85
using
Free Space Wipe 39, 41, 45, 49

V

validating
keys
granting trust for 123
validity
checking a key's 112
verifying
authenticity of a key 112
email 34, 35
VeriSign OnSite 133
viewing
attributes of keyrings 114–118
key attributes 99
volumes
mounting 78
unmounting 79

W

Windows 2000 133
wiping
disks 39, 41, 45, 49
files 39, 45
using Free Space Wipe 39, 45
your smart card 70
word wrap 150

X

X.509 certificates
adding
root CA certificates 132
adding to keypair 124
importing 112